Health and Human Services Agency

CalOHII California Office of Health Information Integrity

California's Statewide Health Information Policy Manual (SHIPM)

Written and Produced by:

California Health and Human Services Agency (CHHS)

California Office of Health Information Integrity (CalOHII)

FINAL: June 25, 2015

Updated: June 1, 2021

Statewide Health Information Policy Manual

Dear SHIPM User:

Welcome to the revised California Statewide Health Information Policy Manual (SHIPM) user community. SHIPM is updated annually after a thorough analysis of enacted legislation and state policy.

This manual was developed and is maintained by the California Health and Human Services Agency's (CHHS) Office of Health Information Integrity (CalOHII).

The SHIPM is an important tool that helps CalOHII fulfill its statutory responsibility to provide statewide leadership, coordination, direction, and oversight of the Health Insurance Portability and Accountability Act (HIPAA) implementation and compliance, including the setting of statewide policy.

Our goal in providing this manual is to offer state departments a resource that:

- Facilitates the appropriate sharing of health information rather than using HIPAA as a barrier,
- Provides departments guidance on how to protect patient privacy while promoting coordinated care,
- Promotes uniform interpretation and application of health information laws including those relating to security, patients' rights, and transactions and code sets, and
- Helps state entities avoid fines and sanctions resulting from unauthorized disclosures of health information.

State entities including all state departments, boards, commissions, programs, and other organizational units of the executive branch of state government that are required to comply with HIPAA must comply with the California SHIPM policies.

For entities not defined by HIPAA as covered entities or business associates, the California SHIPM serves as guidance. These entities may find themselves impacted by HIPAA due to receipt, access, storage, transmission, disclosure, or usage of health information.

State entities are also responsible to know and comply with other legal requirements unique to each state entity and ensure that those provisions are included in the state entity's own policies and procedures, if not already addressed in the SHIPM.

The SHIPM provides direction to help staff working with health information become and remain compliant with HIPAA, as well as other state and federal privacy laws and standards including, but not limited to, the Confidentiality of Medical Information Act (CMIA), the Information Practices Act (IPA), the Lanterman-Petris-Short Act (LPS), the Lanterman Developmental Disabilities Act, the California Penal Code, the California Health and Safety Code, the Patients

Access to Health Records Act (PAHRA), the Genetic Information Nondiscrimination Act (GINA), the California State Administrative Manual (CA SAM), and the National Institute of Standards and Technology (NIST).

CalOHII, with our state department partners, performed legal review of each policy. Preemption analysis was built into the development and review of each policy. If departments impacted by HIPAA (and related laws) follow the SHIPM tenets to develop and manage department-specific policies and procedures, they will help implement and maintain compliance with HIPAA, and the other state and federal laws referenced in the policies.

CalOHII may conduct statutorily-required compliance reviews based on the policies in this manual. Each department impacted by HIPAA and related laws should ensure its internal policies and procedures align with the standards and requirements in the SHIPM.

Finally, we welcome your feedback on the manual. The SHIPM is intended to be a useful, living document that provides on-going guidance and support to HIPAA-impacted state departments. We expect it to be an ongoing, well-used and well-trusted resource. To ensure the SHIPM's ongoing effectiveness, please send any recommended changes to CalOHII for consideration at **OHIcomments@ohi.ca.gov.**

Sincerely,

Elaine Scordakis, MS
Assistant Director
California Office of Health Information Integrity

Table of Contents

How to Use this Manual

Legal Review:

This manual is intended to be a guide for use by those implementing and maintaining department policies relating to health information.

Due to their complex nature, the following policies contain language recommending additional review and interpretation by each department's legal department for guidance in implementation and maintenance of operational policies and procedures:

- Chapter 2: Privacy – Uses and Disclosures – Employers
- Chapter 2: Privacy – Uses and Disclosures – Health Oversight
- Chapter 2: Privacy – Uses and Disclosures – Judicial and Administrative Proceedings
- Chapter 2: Privacy – Uses and Disclosures – Law Enforcement
- Chapter 2: Privacy – Uses and Disclosures – Opportunity to Agree or Object
- Chapter 2: Privacy – Uses and Disclosures – Organ Procurement
- Chapter 2: Privacy – Uses and Disclosures – Public Health Activities
- Chapter 2: Privacy – Uses and Disclosures – Required by Law and Required Disclosures
- Chapter 2: Privacy – Uses and Disclosures – Research
- Chapter 2: Privacy – Uses and Disclosures – Victims of Abuse, Neglect, or Domestic Violence
- Chapter 2: Privacy – Specially Protected Information – HIV/AIDS Information
- Chapter 2: Privacy – Specially Protected Information – Mental Health Records
- Chapter 2: Privacy – Specially Protected Information – Substance Use Disorder Treatment
- Chapter 2: Privacy – Specially Protected Information – Developmental Services Records
- Chapter 2: Privacy – Specially Protected Information – Psychotherapy Notes
- Chapter 2: Privacy – Patient's (Personal) Representative – Patient's (Personal) Representative
- Chapter 3: Security – Administrative Safeguards – Verification of Identity (Person or Entity Authentication)

- Chapter 4: Administrative – Administrative Requirements – Sanctions for Violation
- Chapter 4: Administrative – Business Associates – Business Associate Agreement
- Chapter 5: Patient Rights – Patient Rights – Access - Patient's (Individual's) Right to Access Health Information
- Chapter 5: Patient Rights – Restrictions - Restriction for Self-Pay
- Summary of Privacy Laws

How to Navigate this Document:

- Each policy is linked to the Table of Contents. Using the Control Key and Clicking the policy name/table of contents item will navigate directly to the policy from the Table of Contents.
- Definitions: Definitions associated with the SHIPM policies, are included in the last section of this document. The first time the definition is used in a policy, words and phrases that have SHIPM definitions are hyperlinked to the corresponding definition. The definitions will include the source, citation, and the majority are based on statute. However, definitions might differ from what is familiar because they may include elements of HIPAA, state, and other federal law.
    - All forms of the word are included under one definition (e.g., patient, patients, and patient's would all be listed under "patient" in the definitions)
- Attachments: Attachments to policies on the SHIPM webpage are included as separate documents. Attachment file names on the SHIPM webpage include the policy number for easy reference.

How to Interpret Lists of Items (numbered, lettered, or bulleted):

In the absence of any language to the contrary, assume that it is a list of "OR" items and that the direction applies to each of the items independently.

For example, in the following list, the reader must disclose for any of the following reasons.

Health information shall be disclosed under the following circumstances:

a. By a court pursuant to an order of that court
b. By a board, commission, or administrative agency pursuant to an investigative subpoena
c. By a search warrant lawfully issued to a governmental law enforcement agency

In this example, the reader must disclose health information if requested by a court order OR a subpoena OR a search warrant.

Topic Format:

The format of each chapter and section is consistent from topic to topic. The following summarizes how each policy topic is organized:

I. Purpose

This section briefly states why this policy has been included in the manual and its intended function.

II. Policy

This section contains a clear and explicit general policy statement. Most often, this policy language applies equally to all covered entities, inside or outside state service. Any provisions specific only to state entities are documented in this section.

III. Implementation Specifics

This section provides more specific details on implementing the policy. Occasionally, state entities have additional restrictions or responsibilities beyond those of non-state covered entities due to the Information Practices Act (IPA) or other statutes. These details are identified in this section.

IV. References

This section lists legal citations upon which this policy is based. This includes not only HIPAA, CMIA, California IPA, California Health and Safety Code (CA Health and Safety Code), California Welfare and Institutions Code (CA Welfare and Institutions Code), but also the California State Administrative Manual (CA SAM), National Institute of Standards and Technology (NIST), and other applicable rules.

V. Related Policies

This section identifies related policies, which may help clarify or amplify the current policy. Referenced policies are presented with the SHIPM chapter number and policy name (for example *SHIPM Chapter 4 – Policies and Procedures*).

VI. Attachments

This section lists any documents related to the policy.

Chapter 1 - Overview

Chapter: 1 – Overview		
Section: 1.1.0 – CalOHII Authority		
1.1.1 – CalOHII Authority		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: No

I. Purpose

To summarize the authority and responsibilities of the California Office of Health information Integrity (CalOHII) and ensure full and proper implementation and oversight of the federal Health Insurance Portability and Accountability Act (HIPAA) *and* related state and federal laws.

CalOHII's authority is the basis for this Policy Manual.

II. Policy

California law requires CalOHII to provide statewide leadership, coordination, policy formulation, direction, and oversight for HIPAA implementation, including compliance. CalOHII must also exercise full authority over state entities to establish policy, provide direction, monitor progress, and report on implementation efforts. CalOHII's mandate to provide uniform implementation of HIPAA includes the authority to conduct preemption analyses and set policy based on the results of the analyses.

State entities are responsible for implementing and adopting the policies outlined in the California Statewide Health Information Policy Manual (SHIPM). State entities must cooperate with CalOHII's implementation and compliance efforts, provide documentation or information upon request in the format requested, and assist in periodic statewide assessments to determine which state entities are impacted by HIPAA. State entities must comply with the decisions of CalOHII's Director regarding implementation and compliance with HIPAA standards.

[CA Health and Safety Code § 130303]

III. Implementation Specifics

A. CalOHII Statutory Authority. CalOHII is required to:

1. Specify tools, such as protocols for assessment and reporting.
2. Develop uniform policies and provide training on privacy, security, patient rights, transactions and code sets, and other matters related to HIPAA. These policies must be adopted and implemented by state entities. The policies are also intended to provide a clear understanding of law for state entities that have oversight of other

impacted organizations (such as: state, county, and private-sector), so implementation and enforcement is consistent and accurate.

3. Provide ongoing evaluation of HIPAA implementation in California state departments and to refine plans, tools, and policies as required.
4. Develop standards for state and federal health information law compliance reviews of state departments.
5. Represent the State of California in HIPAA discussions with the U. S. Department of Health and Human Services (HHS) and national and regional groups developing standards.
6. Monitor the HIPAA implementation activities of state entities and require these entities to report on their implementation activities.
7. Provide state entities with technical assistance.
8. Establish and maintain a public website to provide information in a clear, consistent format concerning state HIPAA implementation activities.
9. Review and approve all legislation that is related to administrative aspects of HIPAA, proposed by state entities and review all analyses and positions on HIPAA-related legislation being considered by either the Congress or the Legislature.
10. Ensure state departments claim federal funding for those activities that qualify. *[CA Health and Safety Code § 130306]*

B. Preemption. CalOHII is responsible for leadership, coordination, direction, and oversight regarding HIPAA preemption analyses including determining which statutory requirements apply and setting policy based upon this determination. State entities impacted by HIPAA, at the direction of CalOHII, must assist in completing HIPAA preemption analyses.
[CA Health and Safety Code § 130311.5]

IV. References

CA Health and Safety Code §§ 130300-130317

V. Related Policies

SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter: 1 – Overview		
Section: 1.2.0 – State Agency Responsibility		
1.2.1 - State Agency Responsibility		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding state entity responsibilities, relating to the policies in the State Health Information Policy Manual (SHIPM).

II. Policy

State entities are required to comply with all SHIPM policies and to incorporate the provisions into their own policies and procedures.

III. Implementation Specifics

State entities are responsible to:

A. Know legal requirements unique to each state entity and ensure that those provisions are included in the state entity's own policies and procedures, if not already addressed in the SHIPM.

B. Incorporate the protections, provisions, and requirements of the SHIPM into the state entity's own policies and procedures.
[CA Health and Safety Code § 130303, § 130306, § 130311, and § 130313]

C. Establish procedures describing when to engage legal staff on activities related to specific SHIPM policies, particularly those policies that advise consulting legal counsel.

D. Provide workforce training on SHIPM policies as incorporated into individual state entity policies and procedures as appropriate based on the workforce member's role and responsibilities.
[CA Health and Safety Code § 130311]

E. Provide feedback and comments to California Office of Health information Integrity (CalOHII) regarding SHIPM policies, notices of proposed rule-making, other documents or activities related to Health Insurance Portability and Accountability Act (HIPAA) implementation, compliance, and other state and federal health information privacy and security laws.
[CA Health and Safety Code § 130306]

F. Respond in a timely and complete manner to all activities undertaken to assess and ensure implementation and compliance with SHIPM policies. Responses shall include, but are not limited to:
   1. Assisting in periodic statewide assessments
   2. Assisting in and partnering with periodic compliance reviews
   3. Providing documentation or information upon request in the format requested

   [CA Health and Safety Code § 130306, and § 130310]

G. Comply with the decisions of the CalOHII director in achieving compliance with state and federal health information privacy and security laws.
   [CA Health and Safety Code § 130311]

H. In addition to policies and authorities outlined in SHIPM, state entities must also comply with their own program(s) information security and privacy policies, standards and procedures, as well as those issued by the Office of Information Security (OIS), and the California State Administrative Manual (SAM).
   [CA Government Code § 11549.3; CA SAM §§ 5300 – 5365.3; NIST SP 800-53 Rev. 5]

IV. References

CA Government Code § 11549.3

CA Health and Safety Code

- § 130303
- § 130306
- § 130310
- § 130311
- § 130311.5
- § 130313

CA SAM §§ 5300 – 5365.3

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter 2 – Privacy

Chapter: 2 – Privacy		
Section: 2.1.0 – Authorizations		
2.1.1 – Authorizations		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: Yes

I. Purpose

To provide guidance regarding the circumstances when an authorization for the use and disclosure of health information is required from the patient and what must be included in the authorization.

II. Policy

Patient authorizations are required to permit a state entity that is a covered entity or business associate, to use or disclose health information to an individual/entity for a purpose that would otherwise not be permitted by federal or state privacy regulations.
[45 C.F.R. § 164.508]

For authorization information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

State entities are required to develop, implement, and maintain policies and procedures outlining authorization requirements (when a patient authorization is needed and what must be included).
[45 C.F.R. § 164.508, and § 164.530(i)(1)]

Policies and procedures should address, but not be limited to, the following:

A. Health information can be used or disclosed without authorization for certain specific purposes (*see IV. Related Policies)*.

   All other uses and disclosures of health information require prior authorization from the patient. Authorizations must comply with all HIPAA requirements as well as requirements of the Federal Trade Commission Act (FTC Act).
   [15 U.S.C. § 45(a)]

B. When an authorization is received, uses and disclosures of health information, for the purpose listed in the authorization, are permitted. Business Associates (BA) must ensure they have a valid Business Associate Agreement (BAA), which allows the BA to disclose health information pursuant to an authorization that complies with HIPAA and the FTC Act.
[15 U.S.C. § 45(a); 45 C.F.R. § 164.508]

C. The authorization must be written in plain language, and printed in no smaller than 14-point font. This means that authorizations should be written at an appropriate grade level that most adults can understand.
[45 C.F.R. § 164.508(c)(3); CA Civil Code § 56.11(a), and § 56.17(g)(1)]

D. An authorization must include the following to be valid:
[45 C.F.R. § 164.508(c)]

1. A specific description of the health information to be disclosed.
[45 C.F.R. § 164.508(c)(1)(i); CA Civil Code § 56.10(d), and § 56.17(g)(4)]
2. The types of information listed below must be expressly stated in authorizations:
    a. HIV/AIDS test results (requires a separate authorization for each disclosure)
    [CA Health and Safety Code § 120980(g)]
    b. Mental health records
    [CA Welfare and Institutions Code § 4514(b), § 4514 (d), and § 5328; CA Health and Safety Code § 123115(b)]
    c. Genetic test results (requires a separate authorization for each disclosure)
    [CA Civil Code § 56.17; CA Health and Safety Code § 124980(j)]
    d. Substance use disorder treatment records
    [42 C.F.R. § 2.31; CA Health and Safety Code § 11845.5(c)(4)]

    If a state entity is unclear regarding what health information is covered by the authorization, it must clarify the request prior to disclosing any information.
3. The name or other specific identification of the person(s) or class of persons providing the requested health information.
[45 C.F.R. § 164.508(c)(1)(ii); CA Civil Code § 56.11(e), and § 56.17(g)(3)]
4. The name or other specific identification of the person(s) or class of persons receiving the health information.
[45 C.F.R. § 164.508(c)(1)(iii); CA Civil Code § 56.11(f), and § 56.17(g)(3)]
5. The purpose for the use or disclosure.
    a. If the patient initiates the authorization, the statement “at the request of the patient” or similar language that indicates the patient’s wishes is sufficient description of the purpose.
    [45 C.F.R. §§ 164.508(c)(1)(ii) - (iv)]

b. When someone other than the patient initiates the authorization, the purpose for the use or disclosure of health information must be clear enough to limit use or disclosure to the extent necessary to accomplish the stated purpose.
[45 C.F.R. § 164.502(b)(2)(iii); CA Civil Code § 56.11(h), and § 56.17(g)(7)]

[CA Civil Code § 56.11(d), § 56.11 (g), and § 56.17(g)(6)]

6. An expiration identified by a date. While HIPAA allows for an event as well, the CA Civil Code does not - it allows only a date. When an authorization is signed by a parent, the expiration date of the authorization may be the date the minor reaches age 18.
[CA Civil Code § 56.11(h)]
7. Signature of the patient and date signed. If the authorization is signed by a patient representative, a description of the representative's authority to act for the patient must also be provided.
[45 C.F.R. § 164.508(c)(1)(vi); CA Civil Code § 56.11(c), and § 56.17(g)(2)]
8. Statement that the patient has the right to modify or revoke the authorization in writing, directions on how the patient can do so, and exceptions to the right to revoke.
[45 C.F.R. § 164.508(b)(5), and § 164.508(c)(2)(i)(A)]
9. Statement advising the patient of his/her right to receive a copy of the authorization.
[45 C.F.R. § 164.508(c)(4); CA Civil Code § 56.11(i), § 56.12, and § 56.17(g)(8)]
10. Statement that treatment, payment, enrollment, or eligibility for benefits cannot be conditioned upon patient authorization.
[45 C.F.R. § 164.508(b)(4), and § 164.508(c)(2)(ii)]
11. FTC Act requirements. Authorizations must meet compliance with the FTC Act to ensure information in and surrounding the authorization is not deceptive or misleading.
[15 U.S.C. § 45(a)]
12. HIPAA required statement. Health information disclosed through the authorization may be subject to re-disclosure and is no longer protected if it is disclosed to anyone other than a covered entity.
[45 C.F.R. § 164.508(c)(2)(iii)]

Note: This statement is required by HIPAA even though state entities may not further disclose health information unless through an exception or additional authorization.
[CA Civil Code § 56.10, § 56.11, § 56.13, and § 56.37]

E. Requirements for handling and processing authorizations.

1. Modification or revocation of authorizations. A patient may modify or revoke an authorization at any time in writing. Once notice is received, state entities are responsible for modifying or revoking the authorization based on the patient's request.
   [CA Civil Code § 56.15]
2. Compound authorizations. An authorization for use or disclosure of health information may not be combined with any other document to create a compound authorization.
   [45 C.F.R. § 164.508(b)(3); CA Civil Code § 56.11(b)]
3. Defective (non-valid) authorizations. An authorization is not valid if the document has any of the following defects:
   a. The expiration date has passed
   b. The required elements have not been filled out completely
   c. The authorization is known by the state entity to have been revoked
   d. The authorization violates state or federal law on compound authorizations and/or the prohibition on conditioning of authorizations
   e. Any material information in the authorization is known by the state entity to be false

   [45 C.F.R. § 164.508(b)(2)]

F. Documentation retention. A state entity must retain any authorization, modifications or revocations applied to authorizations for a minimum of six (6) years from date of request.
   [45 C.F.R. § 164.508(b)(6)]

IV. References

15 U.S.C. § 45(a)

42 C.F.R. § 2.31

45 C.F.R.

- §§ 164.502(b) – (b)(2)(iii)
- § 164.508
- § 164.524(c)(3)
- § 164.530(i)(1)

CA Civil Code

- §§ 56.10 – 56.15
- § 56.17
- § 56.37

CA Health and Safety

- § 11845.5(c)(4)
- § 123115(b)
- § 120980(g)
- § 124980(j)

CA Welfare and Institutions

- § 4514(b)
- § 4514(d)
- § 5328

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Uses and Disclosures
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 4 – Business Associate Agreement

VI. Attachments

Yes – Authorization for Release of Information (Template)

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.1 – Decedents		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the privacy rights of deceased patients (decedents) and the requirements to protect the decedent's health information.

II. Policy

Health information of decedents must be protected by all the same safeguards as that of living persons.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) utilized to safeguard health information of decedents.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not limited to, the following:

A. State entities are responsible to:

1. Protect the health information of decedents in the same manner, and to the same extent, as required for the health information of living persons. However, the obligation to protect the health information of decedents is limited to a period of 50 years following the date of the patient's death. After that, the information about the decedent is no longer considered health information.
   [45 C.F.R. § 164.502(f)]
2. Treat executors, administrators or other persons having the authority to act on behalf of decedents or their estates, as the decedents' patient representative, and provide them access to the decedents' health information.

However, such access to health information must be limited to that which is relevant to the authority of each patient representative based on decision by the covered entry or business associate.
[45 C.F.R. § 164.502(g)(4)]

3. Obtain an authorization from a patient representative of decedent for uses or disclosures of decedent's health information not otherwise permitted (*see below*).
[45 C.F.R. § 164.502(g)(4)]

B. Permitted disclosures of a decedent's health information:

1. To alert law enforcement to the death of the patient when there is a suspicion that death resulted from criminal conduct.
[45 C.F.R. § 164.512(f)(4)]

2. To coroners or medical examiners and funeral directors upon request.
[45 C.F.R. § 164.512(g); CA Civil Code § 56.10(c)(13)]

3. For research that is solely on the health information of the decedent.
[45 C.F.R. § 164.512(i)(1)(iii)]

4. To individuals involved in the patient's care, that is relevant to such person's involvement, unless doing so is inconsistent with a prior expressed preference of the individual.
[45 C.F.R. § 164.510(b)]

5. To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.
[45 C.F.R. § 164.512(h); CA Civil Code § 56.10(c)(13)]

Exceptions to the permitted disclosures of decedent's health information. Please *see SHIPM Chapter 2, Specially Protected Information.*

IV. References

45 C.F.R.

- § 164.502(f)
- § 164.502(g)(4)
- § 164.510(b)
- § 164.512(f)(4)
- § 164.512(g)
- § 164.512(h)
- § 164.512(i)(1)(iii)
- § 164.530(i)(1)

CA Civil Code § 56.10(c)(13)
CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Organ Procurement
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Patient's (Personal) Representative
SHIPM Chapter 4 – Policies and Procedures
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.2 – Employers		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the permitted circumstances and required notices that must be provided when health information is disclosed to an employer about a member of the employer's workforce.

II. Policy

Health care providers may disclose the minimum necessary health information, with a valid authorization from the patient, to an employer about a member of the employer's workforce, *or* to itself, as an employer for one of its workforce members.
[45 C.F.R. § 164.512(b)(1)(v)]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) utilized to ensure the minimum amount of health information is disclosed to an employer only with a valid authorization.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are permitted to disclose health information to an employer about a member of the employer's workforce if one of the following conditions are met:
   1. A valid authorization has been obtained from the workforce member *(see SHIPM Chapter 2, Authorizations), or*

2. For payment for health care services. Health information may be disclosed:
   a. To an employer that is not a state agency for payment purposes
   b. To a state agency, for payment purposes if the transfer is necessary for the other state entity to perform constitutional or statutory duties

   [CA Civil Code § 56.10(c)]

   There is an exception to these permitted disclosures for patients who self-pay for health care services *(see SHIPM Chapter 5, Restriction for Self-Pay).*

B. When required by law, the disclosure of health information is permitted for:
   1. Occupational Safety and Health Administration (OSHA)/CalOSHA reporting
   2. Public Health reporting
   3. Workers' Compensation subpoena

   Consult with your legal counsel before developing policies and procedures, or disclosing health information in response to a Workers' Compensation subpoena.

   [45 C.F.R. § 164.512(b)(1)(v), and § 164.512(l); CA Civil Code § 56.10(c)(18), and § 1798.24]

C. State entities are permitted to disclose health information *internally* about a member of the state entity's workforce, for the purpose of:
   1. Reasonable accommodation and return to work laws
   2. Workers' Compensation laws
   3. OSHA/CalOSHA laws
   4. Legal defense *(consult with your legal counsel*)

   [CA Civil Code § 56.30]

IV. References

45 C.F.R.

- § 164.512(b)(1)(v)
- § 164.512(l)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(c)
- § 56.30
- § 1798.24

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 5 – Restriction for Self-Pay

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.3 – Fundraising		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the circumstances under which health information may be used or disclosed for fundraising purposes.

II. Policy

A valid authorization must be obtained from the patient prior to using or disclosing health information for fundraising purposes.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

A. While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) used to prevent fundraising activities using health information without a valid authorization.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

B. State entities cannot use or disclose health information for fundraising activities without obtaining a valid authorization from the patient.
[45 C.F.R. § 164.514(f); CA Civil Code § 1798.24]

IV. References

45 C.F.R.

- § 164.514(f)
- § 164.530(i)(1)

CA Civil Code § 1798.24

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Specially Protected Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.4 – Health Oversight		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding uses or disclosures of health information for health oversight purposes.

II. Policy

Health information is permitted to be used by, and disclosed to government agencies that are legally authorized to conduct health oversight activities, if such activities are necessary for the appropriate operation and management of programs, and other functions involving the provision of health care or health care related services.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.
[45 C.F.R. § 164.512(d); CA Civil Code §§ 56.10(c)(2) – (c)(7), § 56.10(c)(14), and § 1798.24]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information to government agencies performing health oversight activities.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are responsible to:
   1. Understand what constitutes health oversight activities, and how to respond to requests for health information by other agencies for this purpose.
   2. Limit disclosure of health information to the minimum necessary for the stated health oversight purpose.
   3. Be prepared to address health information privacy concerns of other state entities when requesting health information.
   4. Require reasonable evidence and/or legal authority in the forms listed below:
      a. A written statement of identity on agency letterhead
      b. An identification badge
      c. Similar proof of official status, *or*
      d. Written request provided on agency letterhead describing legal authority for release of health information.
   5. Understand that health oversight agency representatives will be required to provide verification of both identity and authority when requesting health information for authorized oversight activities.

B. Permitted uses. A state entity that is also a health oversight agency may use health information (internally) for health oversight activities.
[45 C.F.R. § 164.512(d)(4)]

C. Permitted disclosures. Health information may be disclosed to a health oversight agency, without an authorization, for authorized oversight activities (examples include, but are not limited to, audits, licensure or disciplinary actions).
[45 C.F.R. § 164.512; CA Civil Code § 56.10, and §§ 1798.24 –1798.25]

D. Exceptions to permitted disclosures to health oversight agencies. A health oversight activity *does not include* an investigation or other activity in which the patient is the subject of the investigation or activity, when it is not a direct result of, or directly related to:
   1. The receipt of health care
   2. A claim for public benefits related to health
   3. Qualification for, or receipt of, public benefits or services when a patient's health is vital to the claim for public benefits or services
   4. Reporting of child abuse, neglect, or domestic violence (*see SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence*)
   5. Payment collection activities related to provision of health care *(see SHIPM Chapter 2, Treatment, Payment and Health Care Operations)*

[45 C.F.R. § 164.512(d)]

E. Temporary suspension of accounting of disclosures. Health oversight agencies may request a temporary suspension of a patient's right to receive an accounting of disclosures. The temporary suspension must be made in writing, include the reason why the disclosure would impede the health oversight activities and indicate the time frame the suspension is required.

For requests made orally, the patient's right to an accounting will be suspended for no more than 30 days unless a written request is submitted during that timeframe.
[45 C.F.R. § 164.528]

F. Joint activities or investigations. If a health oversight activity is conducted in conjunction with a public benefits investigation (not related to health), the joint activity or investigation is considered a health oversight activity (e.g., Social Security Number fraud involving health treatment and other public benefits such as food stamps, housing vouchers, etc.).
[45 C.F.R. § 164.512(d)(3)]

G. Notice of Privacy Practices. A state entity that is a business associate, health care clearinghouse, health care plan, health care provider, or hybrid entity, must state in its Notice of Privacy Practices, if applicable, that it will disclose health information to health oversight agencies for health oversight purposes. Some entities are exempt, *see SHIPM Chapter 5, Notice of Privacy Practices*.
[45 C.F.R. § 164.504(e)]

IV. References

45 C.F.R.

- § 164.501
- § 164.504(e)
- § 164.512
- § 164.528
- § 164.530(i)(1)

CA Civil Code

- § 56.10
- §§ 1798.24 – 1798.25

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)

SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.5 – Judicial and Administrative Proceedings		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the permitted uses and disclosures of health information for purposes of administrative and judicial proceedings.

II. Policy

Health information shall be disclosed in the course of a judicial or administrative proceeding without a patient authorization if disclosure is compelled, such as in response to a court order, valid subpoena, or other compulsory legal process.

However, prior to disclosing the information, state entities are responsible for reasonably attempting to notify the patient who is the subject of the compelled information, if the notification is not prohibited by law.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.

Due to the nature, complexity, and sensitivity of this area, state entities should consult with their legal counsel before disclosing health information in response to subpoenas or when developing and implementing operational policies and procedures.
[45 C.F.R. §§ 164.512(e)(1) – (e)(2); CA Civil Code § 1798.24]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information related to a judicial or administrative proceeding.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities shall disclose health information to the extent necessary, without an authorization, after reasonably attempting to notify the patient in writing. State entities are responsible for maintaining the notification documentation for a minimum of six (6) years.

B. Health information shall be disclosed under the following circumstances:
   1. By a court pursuant to an order of that court.
   2. By a party to a proceeding before a court or administrative agency, pursuant to a subpoena, notice to appear, or any provision authorizing discovery, in a proceeding before a court or administrative agency.
      [CA Code of Civil Procedure § 1987; CA Civil Code § 1798.24(k)]
   3. By a board, commission, or administrative agency pursuant to an investigative subpoena.
      [CA Government Code § 11180]
   4. By an arbitrator or arbitration panel, when arbitration is lawfully requested by either party, pursuant to a subpoena, in a proceeding before an arbitrator or arbitration panel.
      [CA Code of Civil Procedure § 1282.6]
   5. By a search warrant lawfully issued to a governmental law enforcement agency.
   6. By the patient or the patient's representative.
      [CA Health and Safety Code § 123100]
   7. When responding to requests otherwise specifically required by law *(see SHIPM Chapter 2, Required by Law and Required Disclosures).*
   8. When responding to an investigative subpoena issued by a law enforcement entity *(see SHIPM Chapter 2, Law Enforcement)*.

[45 C.F.R. §§ 164.512(e)(1)(i) – (e)(1)(ii); CA Civil Code § 56.10(b), and § 1798.24]

IV. References

45 C.F.R.

- § 164.512(e)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(b)
- § 1798.24

CA Code of Civil Procedure

- § 1282.6
- § 1987

CA Government Code § 11180

CA Health and Safety Code

- § 123100
- § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Uses and Disclosures – All
SHIPM Chapter 2 – Specially Protected Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.6 – Law Enforcement		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the requirements for disclosure of health information for law enforcement purposes.

II. Policy

Health information may be disclosed, without an authorization from the patient, for law enforcement purposes to law enforcement officials, provided certain conditions are met.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.

Due to the nature, complexity, and sensitivity of this area, state entities are encouraged to consult with their legal counsel before disclosing health information to law enforcement or developing and implementing operational policies and procedures.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information for law enforcement purposes.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are required to disclose health information to law enforcement officials in response to the following:

1. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer.
   [45 C.F.R. § 164.512(f)(1)(ii)(A); CA Civil Code § 56.10(b); CA Penal Code §§ 1543 - 1545]
2. A grand jury subpoena.
   [45 C.F.R. § 164.512(f)(1)(ii)(B)]
3. An administrative request, including an administrative subpoena or summons; a civil or an authorized investigative demand; or similar process authorized under law provided that:
   a. The information sought is relevant and material to a legitimate law enforcement inquiry
   b. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought
   c. De-identified information could not reasonably be used
   d. The request, or a separate document, indicates that the requirements (*Items #3, a-c above*) have been satisfied

   [45 C.F.R. § 164.512(f)(1)(ii)(C)]
4. Identification and location purposes. State entities are permitted to disclose health information in response to a law enforcement official's written or oral requests for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person limited to the following information:
   a. Name and address
   b. Date and place of birth
   c. ABO blood type and Rh factor
   d. Social Security Number
   e. Type of injury
   f. Date and time of treatment
   g. Date and time of death (if applicable)
   h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos

   [45 C.F.R. § 164.512(f)(2)(i)]
5. Victims of a crime. When not otherwise required by law, disclosure of health information in response to a law enforcement official's written or oral request for information about a patient who is or suspected to be the victim of a crime is permitted if:

a. The patient agrees to the disclosure

b. The patient's agreement cannot be obtained because of incapacity or other emergency circumstances, provided that all of the following are met:

   i. The law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred, and that the information is not intended to be used against the victim,

   ii. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure, *and*

   iii. The disclosure is in the best interests of the patient as determined by the entity making the disclosure.

c. If it is suspected that the patient may be a victim of child abuse or neglect, elder abuse or neglect, or domestic violence *(see SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence).*

[45 C.F.R. § 164.512(f)(3)]

6. Decedents. Disclosure of health information to a law enforcement official about a patient who has died if there is suspicion that death may have resulted from criminal conduct *(see SHIPM Chapter 2, Decedents)*.
   [45 C.F.R. § 164.512(f)(4)]

7. Crime on the premises. Disclosure of health information to a law enforcement official if there is a reasonable and honest belief that it constitutes evidence of criminal conduct.
   [45 C.F.R. § 164.512(f)(5)]

8. During an emergency. If a state entity that is a covered health care provider is providing emergency health care in response to a medical emergency that is not on its own premises, then disclosure of health information is permitted to a law enforcement official if doing so appears necessary to alert the law enforcement official to:

   a. The commission and nature of a crime,

   b. The location of such crime or of the victim(s) of such crime, and

   c. The identity, description, and location of the perpetrator of such crime.

   If the state entity believes that the medical emergency is the result of abuse, neglect, or domestic violence of the patient in need of emergency health care, see *SHIPM Chapter 2, Victims of Abuse, Neglect or Domestic Violence*.
   [45 C.F.R. § 164.512(f)(6)(i), and § 164.512(f)(6)(ii)]

IV. References

45 C.F.R.

- §§ 164.512(f)(1) – (f)(6)
- § 164.530(i)(1)

CA Civil Code § 56.10(b)

CA Health and Safety Code § 130303

CA Penal Code §§ 1543 – 1545

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Decedents
SHIPM Chapter 2 – Judicial and Administrative Proceedings
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.7 – Marketing		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

For guidance regarding the uses and disclosures of health information for marketing purposes.

II. Policy

State entities cannot use or disclose health information for marketing purposes.

Enforcement agencies are responsible for ensuring that health information obtained from state entities is not used or disclosed for marketing purposes, unless a valid, written authorization has been obtained from the patient.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

A. Policies and procedures. Enforcement entities are responsible for maintaining policies and procedures that outline the details and restrictions of marketing activities.

Though not required, it is a best practice to include this information in the state entity's Notice of Privacy Practices (see SHIPM Chapter 5, Notice of Privacy Practices).
[45 C.F.R. § 164.316(a)]

B. Guidance to enforcement entities. Health information obtained from state entities may not be used or disclosed for marketing purposes without a valid, written authorization from the patient.

A valid authorization for marketing must contain the following information:

1. The fact that the state entity is receiving a financial benefit from a third party, if applicable.
2. Adequate descriptions of the intended purposes of the requested uses and disclosures and the scope of the authorization.

3. A clear statement that the patient may revoke the authorization at any time.
   [45 C.F.R. § 164.501, and § 164.508(a)(3); CA Civil Code §§ 56.10 - 56.16]
4. It must also comply with the SHIPM Authorization policy (*see SHIPM Chapter 2, Authorizations*).
   [45 C.F.R. § 164.508(a)(3); CA Civil Code § 56.10(d)]

C. Exceptions to required authorizations. The following are exceptions and *do not* require an authorization, because they do not meet the definition of marketing:

1. Refill reminders, or other communications about a drug or biologic currently being prescribed to a patient. Federal law permits state entities to receive payment for these communications as long as the amounts received are reasonably related to the cost of creating the communication and include only the costs of labor, supplies, and postage to make the communication.

   Examples include, but are not limited to:

   a. A pharmacy emails a patient of the need to refill their prescription
   b. A pharmacy sends a letter to a patient that the patient is running out of refills and to see their provider for renewal
   c. A pharmacy calls a patient to inform them medication is available for pickup

   [42 U.S.C. § 17936(a)]
2. General communications that are deemed necessary to promote health without promoting a particular provider‘s services or products.
3. Communications about government and government-sponsored programs (as long as they do not include a commercial component).
   [45 C.F.R. § 164.501, and § 164.508(a)(3); CA Civil Code § 56.10(d), and § 56.11]
4. General communications necessary to ensure appropriate treatment for a patient.

   Examples include but are not limited to:

   a. A provider texts a patient to remind the patient to take prescribed medication
   b. A pharmacy calls a provider to inform the provider that the patient did not refill their medication so the provider can determine whether to provide counseling
   c. A lab contacts a provider to inform the provider that test results indicate low or non-existent levels of medication
   d. A provider reviews lab results indicating low or non-existent levels of medication and calls a patient for counseling

D. Business associates. If a business associate (BA) conducts marketing activities, the business associate agreement must explicitly limit the BA to only communications by the business associate using health information to those approved by, and on behalf of, the state entity.
[45 C.F.R. § 164.508(a)(3)]

IV. References

42 U.S.C. § 17936(a)

45 C.F.R.

- § 164.316(a)
- § 164.501
- § 164.508(a)(3)

CA Civil Code §§ 56.10 – 56.16

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 4 – Policies and Procedures
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.8 – Opportunity to Agree or Object		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding a patient's opportunity to agree or object to certain uses or disclosures of his or her health information.

II. Policy

State entities are responsible to inform the patient in advance, if practicable, about their opportunity to agree or object to uses or disclosures of their health information.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.
[45 C.F.R. § 164.510]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to allow patients the opportunity to agree, or object to specific uses and disclosures of their health information.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Patient's prior preference. If the state entity knows of a patient's prior expression of preference, the state entity must follow that expression. This may involve disclosing some portion of the patient's health information but not others, to comply with the patient's preferences.

B. Uses and disclosures - with the patient present. If the patient is present for, or otherwise available prior to, a permitted use or disclosure and has the capacity to make health care decisions, the state entity may use or disclose the health information *if* it:

1. Obtains the patient's agreement
2. Provides the patient with the opportunity to object to the disclosure, and the patient does not express an objection
3. Reasonably infer from the circumstances, that the patient does not object to the disclosure

[45 C.F.R. § 164.510(b)(2)]

C. Uses and disclosures - when the patient *is not* present. If the patient is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the patient's incapacity or an emergency circumstance, the state entity may determine whether the disclosure is in the best interests of the patient and, if so, disclose the minimum necessary that is directly relevant to the person's or entity's involvement with the patient's care or payment related to the patient's health care or necessary for notification purposes.

A state entity may use its experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of health information.

[45 C.F.R. § 164.510(b)(3)]

D. Disclosure for facility directories. State entities are responsible for informing patients they may be included in a facility directory, how the directory may be used, and the persons to whom the state entity may disclose the health information in the directory. Any of the following may be used to maintain a directory of patients in a health care facility:

1. The patient's name
2. The patient's location in the facility
3. The patient's condition described in general terms that does not communicate specific health information about the patient
4. The patient's religious affiliation. If a patient provides such information, the state entity may release that information only to clergy members and not to other persons. A state entity must provide patients with the opportunity to prohibit or restrict some or all of these uses or disclosures

[45 C.F.R. § 164.510(a)(1)(ii), and § 164.510(a)(2)]

5. In emergencies. Patients may not be able to object because they are incapacitated or receiving emergency treatment. If the opportunity to object cannot practicably be provided because of patient incapacitation or receipt of emergency treatment, the state entity may use or disclose health information for the facility's directory, if such disclosure is either of the following:
   a. Consistent with a prior expressed preference of the patient, if any, that is known to the state entity
   b. It is in the patient's best interest as determined by the state entity

   The state entity must inform the patient and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

E. Involvement in the patient's care and for notification purposes. A state entity may disclose to a family member, other relative, close personal friend of the patient, or any other person *identified by the patient,* the health information directly relevant to such person's involvement with the patient's health care, or payment related to the patient's health care.
[45 C.F.R. § 164.510(b)(1)(i)]

1. A state entity may use or disclose health information to notify, or assist in the notification of (including identifying or locating), a family member, a representative of the patient, or another person responsible for the care of the patient of the patient's location, general condition, or death.
   [45 C.F.R. § 164.510(b)(1)(ii)]
2. If the patient is deceased, such uses or disclosures may be made unless doing so is inconsistent with any prior expressed preference of the patient that is known to the state entity. A power of attorney or other legal relationship to a patient is not necessary for these disclosures.
   [45 C.F.R. § 164.510(b)(5)]
3. State entities are not required to verify the identity of relatives or other persons involved in the patient's care. However, it is recommended that state entities confirm with the patient that he or she authorizes disclosing health information while the other person is present.
   [45 C.F.R. § 164.514(h)]

F. For disaster relief purposes. A state entity may use or disclose health information to a public or private entity, authorized by law or its charter to assist in disaster relief efforts, to notify or assist in the notification of the patient's location, general condition, or death to any of the following persons:

1. A family member
2. A patient representative
3. Another person responsible for the patient's care

[45 C.F.R. § 164.510(b)(4)]

G. Documentation retention. Patients may be informed of, and may agree or object to the proposed use or disclosure orally, but any prohibition or restriction by patients must be documented and maintained for at least six (6) years.
[45 C.F.R. § 164.510]

IV. References

45 C.F.R.

- § 164.510
- § 164.514(h)
- § 164.530(i)(1)

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Public Health Activities
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Patient's (Personal) Representatives
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 4 – Waiver of Rights Related to HIPAA Complaints
SHIPM Chapter 5 – Restriction for Self-Pay

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.9 – Organ Procurement		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the permitted uses and disclosures of health information for organ procurement purposes.

II. Policy

A patient's health information may be disclosed, without an authorization, to a coroner, medical examiner, forensic pathologist, or organ or tissue banks, upon request, for the purpose of facilitating organ, eye, tissue donation, or transplantation.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.
[45 C.F.R. § 164.512(h); CA Civil Code § 56.10(b)(8), § 56.10(c)(13), and § 1798.24(i)]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose a deceased patient's health information for organ procurement.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303*]*

Policies and procedures should address, but not be limited to, the following:

A. State entities *must* disclose without delay health information of the deceased donor to a coroner, medical examiner, or forensic pathologist upon request for either of the following:

1. For the purpose of organ or tissue donation
2. Upon notification or investigation of imminent deaths that may involve organ or tissue donation

[CA Health and Safety Code § 7151.15; CA Civil Code § 56.10(b)(8)]

B. State entities may disclose health information to organ procurement or tissue bank organizations processing the tissue of a donor for transplantation into the body of another person. However, only the donor's information may be disclosed for the purpose of aiding the transplant.
[45 C.F.R. § 164.512(h); CA Civil Code § 56.10(b)(8), § 56.10(c)(13), and § 1798.24(i); CA Health and Safety Code § 1644, and §§ 7181 – 7184.5]

C. State entities that are acute care hospitals, may disclose health information to next of kin of a deceased person to notify them of the option for organ donation.
[CA Health and Safety Code § 7184]

IV. References

45 C.F.R.

- § 164.512(h)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(b)(8)
- § 56.10(c)(13)
- § 1798.24(i)

CA Health and Safety Code

- § 1644
- § 7151.15
- §§ 7181 – 7184.5
- § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Decedents
SHIPM Chapter 2 – Specially Protected Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.10 – Public Health Activities		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding disclosures of health information to public health authorities.

II. Policy

Health information *must* be disclosed to public health authorities, without a patient's authorization, when required by law.

Health information *may* be disclosed for public health activities, without the patient's authorization, when the reason for the disclosure is related to the purpose for which the information was collected and under the circumstances outlined under "*Implementation Specifics*."

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.
[45 C.F.R. § 164.512(b); CA Civil Code § 1798.24]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information for public health activities.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities may disclose health information to public health authorities who are legally authorized to receive such reports to prevent or control disease, injury, or disability. This includes, but is not limited to, any of the following:

   1. The reporting of a disease or injury
   2. Reporting vital events, such as births or deaths
   3. Conducting public health surveillance, investigations, or interventions

   [45 C.F.R. § 164.512(b)(1)(i); CA Civil Code § 56.10(c), and § 1798.24]

B. State entities that are public health authorities may use and disclose health information for public health purposes, if specifically authorized by law.
   [45 C.F.R. §§ 164.512(b)(1) - (2); CA Civil Code § 56.10(c)(14), and § 1798.24]

C. Health information may be disclosed as needed to notify a person that (s)he has been exposed to a communicable disease, or is at risk of contracting or spreading a disease or condition, if the state entity is legally authorized to do so to prevent or control the spread of the disease.
   [45 C.F.R. § 164.512(b)(1)(iv)]

D. Verification of identity. State entities are responsible for verifying public health authorities' status and identity *(see SHIPM Chapter 3, Verification of Identity).*
   [45 C.F.R. § 164.514(h)]

E. Minimum Necessary. State entities are responsible for reasonably limiting the health information disclosed for public health purposes to the minimum necessary to accomplish the intended purpose *(see SHIPM Chapter 2, Minimum Necessary)*.

   However, state entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to a patient's authorization or for disclosures that are required by law.
   [45 C.F.R. § 164.502(b)]

F. Accounting of disclosures. State entities are responsible to document, track and maintain information concerning disclosures of health information. This tracking must document what, when, why and to whom disclosures are made (*see SHIPM Chapter 5, Accounting of Disclosures)*.

IV. References

45 C.F.R

- § 164.502(b)
- § 164.512(b)
- § 164.514(h)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(c)
- § 1798.24

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.11 – Required by Law and Required Disclosures		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding required uses or disclosures of health information, which are mandated by federal or state law.

II. Policy

Health information must be disclosed when required by state or federal law, and limited to the extent required by law.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information when required or mandated by law.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are responsible for identifying laws and regulations that require disclosures of health information, and limiting any uses or disclosures *only* to what is necessary to comply with the law.

B. Prior to disclosure of health information, state entities are responsible to verify the identity and authority/credentials of the requestor (*see SHIPM Chapter 3, Verification of Identity*).

C. For state entities that are business associates, health care clearinghouses, health care plans, health care providers, or hybrid entities, disclosures are required under any of the following circumstances:

1. When oversight requires health information to determine compliance with the Privacy Rule.
2. By court order.
   [CA Civil Code § 56.10(b)(1)]
3. By a board, commission, or administrative agency for adjudication.
   [CA Civil Code § 56.10(b)(2)]
4. By a warrant, subpoena, or summons issued by the court. This includes a subpoena to produce evidence, a notice to appear which has been served, or any provision authorizing discovery in a proceeding before a court or administrative agency.
   [CA Civil Code § 56.10(b)(3)]
5. By a board, commission, or administrative agency pursuant to an investigative subpoena.
   [CA Civil Code § 56.10(b)(4)]
6. By an arbitrator or arbitration panel, to produce specific documentation, in a proceeding before an arbitrator or arbitration panel.
   [CA Civil Code § 56.10(b)(5)]
7. By a search warrant issued to a law enforcement agency.
   [CA Civil Code § 56.10(b)(6)]
8. By the patient or the patient's representative.
   [45 C.F.R. § 164.502(a)(2)(i); CA Civil Code § 56.10(b)(7)]
9. By a coroner, medical examiner, or forensic pathologist, when requested in the course of an investigation by the coroner's office to identify a deceased person, determine cause of death, or other duties approved by law.
   [CA Civil Code § 56.10(b)(8)]
10. To the U.S. Department of Health and Human Services (HHS), when disclosure is required to investigate and determine a state entity’s compliance with HIPAA, with disclosure limited to information pertinent to determine compliance.
    [45 C.F.R. § 164.502(a)(2)(ii)]
11. When otherwise specifically required by law.
    [CA Civil Code § 56.10(b)(9)]

D. Special requirements. State entities are responsible to follow special procedures regarding the following disclosures:

1. About victims of abuse, neglect, or domestic violence
2. For judicial/administrative proceedings/subpoena
3. For law enforcement purposes

See SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence; Judicial and Administrative Proceedings; and Law Enforcement, regarding uses and disclosures for these required disclosures.

E. Minimum necessary. When the law requires a use or disclosure, the HIPAA minimum necessary rule does not apply. However, a best practice is to limit uses and disclosures to the information requested that is relevant and material to the inquiry.

IV. References

45 C.F.R.

- § 164.502
- § 164.530(i)(1)

CA Civil Code § 56.10

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Judicial and Administrative Proceedings
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 3 – Verification of Identity

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.12 – Research		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To describe the permitted uses and disclosures of protected health information for research purposes.

II. Policy

A patient's health information may be disclosed without a patient authorization for purposes of research, under specific circumstances described below or with an authorization that contains a sufficient description of the purpose of the use or disclosure.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.

Due to the nature, complexity, and sensitivity of this area, state entities are advised to consult with their legal counsel before disclosing health information for research purposes or developing and implementing operational policies and procedures.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for research purposes.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Use and disclosure without patient authorization. State entities are permitted to disclose health information to the University of California, a nonprofit educational institution, or in the case of education-related data - another nonprofit entity, conducting scientific research, if the request is approved by either of the following:

1. By the California Health and Human Services Agency (CHHS) Committee for the Protection of Human Subjects
2. By a legally authorized institutional review board (IRB)

[45 C.F.R. § 164.512(i); CA Civil Code § 1798.24(t)]

B. Use of de-identified information. A patient's health information that has been de-identified may be used or disclosed for research purposes *(see SHIPM Chapter 2, De-identification)*.

C. Use of a limited data set. A patient's health information that is part of a limited data set may be used or disclosed for research purposes, if the state entity enters into a data use agreement with the recipient of the health information *(see list in SHIPM Chapter 2, De-identification).*

For this policy, a data use agreement is defined as an agreement entered into by a covered entity and a researcher, pursuant to which the covered entity may disclose a limited data set of health information to the researcher for research, public health, or health care operations.

[45 C.F.R. § 164.514(e); CA Civil Code § 1798.24(t)]

D. Accounting of disclosures. Upon request by the patient, state entities are responsible for providing an accounting of disclosures related to research for the six (6) years prior to the request (*see SHIPM Chapter 5, Accounting of Disclosures*).

[45 C.F.R. § 164.528]

IV. References

45 C.F.R.

- § 164.508(c)
- § 164.512(i)
- § 164.514
- § 164.528
- § 164.530(i)(1)

CA Civil Code

- § 56.10(c)(7)
- § 1798.24(t)

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 5 – Accounting of Disclosures

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.13 – Specialized Government Functions		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the permitted uses and disclosures of health information for specialized government functions.

II. Policy

Health information may be disclosed, without a patient authorization, when the use or disclosure involves, or is related to, a specialized government function defined below.

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information for specialized government functions.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are permitted to disclose health information, without patient authorization, for any of the following specialized government functions:
   1. Correctional institutions and other law enforcement custodial situations. If the disclosure of health information is made to authorized correctional or law enforcement officials with lawful custody of the patient, *and* the health information is needed, according to the law enforcement official or representatives of the correctional institution, to do any of the following:
      a. Provide health care to the patient
      b. Ensure the health and safety of the patient or other inmates

c. Ensure the health and safety of officers, employees, or others at the correctional institution
d. Ensure the health and safety of individuals responsible for transporting or transferring of patient inmates from one institution, facility, or setting to another
e. Enforce the law on the premises of the correctional institution
f. Administer and maintain the safety, security, and good order of the correctional institution

[45 C.F.R. § 164.501, § 164.512(j), § 164.512(k)(5), and § 164.514(h); CA Civil Code § 56.10(c)(14), and §§ 1798.24(d) – (f)]

2. Government programs providing public benefits. Health information is permitted to be disclosed when the disclosure is related to the purpose for which the information was collected, *and* any of the following:
   a. The state entity is a health care plan that is a government program
   b. The disclosure is to another entity administering a government program providing public benefits
   c. The disclosure is required or expressly authorized by law, and
      i. The disclosure is the sharing of eligibility or enrollment information
      ii. Is required for the maintenance of information in a single or combined data system accessible to both government agencies

   [45 C.F.R. §§ 164.512(k)(1) - (k)(6), and § 164.514(h); CA Civil Code § 56.10, and § 1798.24]

3. Government agencies administering a government program providing public benefits. Health information is permitted to be disclosed when the disclosure is related to the purpose for which the information was collected, *and* any of the following:
   a. The state entity is a covered entity administering a government program providing public benefits
   b. The disclosure is to another covered entity that is a government agency administering a government program providing public benefits
   c. Both programs serve the same or similar populations
   d. The disclosure is necessary to coordinate HIPAA covered functions of the programs, or to improve administration and management relating to the programs covered functions

   [45 C.F.R. §§ 164.512(k)(1) - (k)(6), and § 164.514(h); CA Civil Code § 56.10, and § 1798.24]

4. Military and veterans activities. Disclosure of health information of armed forces personnel is permitted, *if* upon separation or discharge from military service, disclosure is made by a component of the Departments of Defense or Homeland Security to provide information to the Department of Veterans Affairs (DVA) to determine eligibility for benefits.
   [45 C.F.R. § 164.500(c), § 164.512(k)(1), and § 164.514(h)]

5. National security and intelligence activities. If the disclosure of health information is made to authorized federal officials conducting lawful intelligence, counter intelligence and other national security activities authorized by the National Security Act, *and* the disclosure is any of the following:
   a. Required by law
   b. Compelled due to circumstances affecting the health or safety of an individual
   c. Compelled through subpoena or warrant
   [45 C.F.R. § 164.512(k)(2), and § 164.514(h); 50 U.S.C. § 401 (and implementing authority e.g., U. S. Executive Order 12333); CA Civil Code § 1798.24(i)]

6. Protective services for the President and others. If the disclosure of health information is made to authorized federal officials to protect the President and other persons, including foreign heads of state, or to conduct investigations authorized by United States Code, *and* the disclosure is any of the following:
   a. Required by law
   b. Compelled due to circumstances affecting the health or safety of an individual
   c. Compelled through subpoena or warrant
   [45 C.F.R. § 164.512(k)(3), and § 164.514(h); 18 U.S.C. § 871, § 879, and § 3056; 22 U.S.C. § 2709(a)(3); CA Civil Code § 1798.24(i)]

B. State entities are responsible to verify the identity of federal officials or correctional and law enforcement representatives *(see SHIPM Chapter 3, Verification of Identity).*

C. State entities are responsible for ensuring that only the minimum amount of health information necessary to achieve the purpose is disclosed *(see SHIPM Chapter 2, Minimum Necessary)*.

D. Accounting of disclosures. State entities are responsible to document, track and maintain information concerning disclosures of health information. This tracking must document what, when, why and to whom disclosures are made (*see SHIPM Chapter 5, Accounting of Disclosures)*.

IV. References

18 U.S.C.

- § 871
- § 879
- § 3056

22 U.S.C. § 2709(a)(3)

50 U.S.C. § 401

45 C.F.R.

- § 164.500(c)
- § 164.501
- § 164.512(j)
- §§ 164.512(k)(1) – (k)(6)
- § 164.514(h)
- § 164.530(i)(1)

CA Civil Code

- § 56.10
- § 1798.24

CA Health and Safety Code § 130303

U. S. Executive Order 12333

Foreign Services Act

- § 101(a)(4)
- § 101(b)(5)
- § 504(t)
- § 904

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Organ Procurement
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.14 – Treatment, Payment and Health Care Operations (TPO)		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding uses or disclosures of health information for the purposes of treatment, payment, or health care operations (TPO).

II. Policy

Health information may be used or disclosed, without a patient authorization, to facilitate TPO when it is collected for the purpose of providing health care services.

Health information may *NOT* be used or disclosed, without a patient authorization, for TPO if it was collected for another purpose, not related to health care services.
[45 C.F.R § 164.506; CA Civil Code § 56.10, and § 1798.24]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for TPO.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Health information may be used or disclosed, without a patient authorization, to facilitate TPO when it is collected for the purpose of providing health care services, as detailed below:
   1. State entities may use and disclose health information to a covered entity, business associate, health care clearinghouse, health care plan, health care provider, or hybrid entity, without a patient authorization for TPO activities as follows:

a. For treatment. State entities may disclose health information for either of the following:

   i. The provision, coordination, or management of health care and related services among health care providers, consultation between providers regarding a patient, or patient referrals from one provider to another.
   [45 C.F.R. § 164.501; CA Civil Code § 56.10(c)(1)]

   ii. Its own treatment activities and the treatment activities of another health care provider.
   [45 C.F.R. §§ 164.506(c)(1) – (c)(2)]

b. For payment. State entities may use health information for their own payment activities and may disclose health information for the payment activities of the entity (entities described in III.A.1. above) receiving the information, as follows:
   [45 C.F.R. §§ 164.506(c)(1) – (c)(2)]

   To an insurer, employer, health care service plan, hospital service plan, employee benefit plan, governmental authority, business associate, or any other person or entity responsible for paying for health care services including a person or entity that provides billing, claims management health data processing, or other administrative services to health care providers, health care service plans, or any of the persons or entities specified above *to the extent necessary* to allow responsibility for payment to be determined and made.
   [CA Civil Code § 56.10(c)(2), and § 56.10(c)(3)]

c. For health care operations. State entities may use health information for health care operations and may disclose health information to another entity (entities described in III.A.1. above) if both of the following are met:

   i. Each entity has or had a treatment relationship with the patient who is the subject of the requested health information

   ii. The health information pertains to that treatment relationship, and the disclosure is for one of the following purposes:

      1. Conducting quality assessment and improvement activities
      2. Evaluating provider performance
      3. Health care fraud and abuse detection or compliance

   [45 C.F.R. § 164.506(c)(1), and § 164.506(c)(4); CA Civil Code § 56.10(c)]

2. Additional restrictions exist when sharing health information between state entities. State entities may use and disclose health information, without a patient authorization, for TPO to another state entity only if necessary for the other state entity to perform constitutional or statutory duties compatible with providing health care services.

IV. References

45 C.F.R.

- § 164.501
- § 164.506
- § 164.530(i)(1)

CA Civil Code

- § 56.10
- § 1798.24

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 - CalOHII Authority
SHIPM Chapter 2 - Authorizations
SHIPM Chapter 2 - Law Enforcement
SHIPM Chapter 2 - Opportunity to Agree or Object
SHIPM Chapter 2 - Required by Law and Required Disclosures
SHIPM Chapter 2 - Victims of Abuse, Neglect or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 - Minimum Necessary
SHIPM Chapter 2 - Patient's (Personal) Representatives
SHIPM Chapter 5 - Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.15 – Underwriting		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding when health information can be used or disclosed for underwriting purposes, without the patient's permission (authorization or consent).

II. Policy

Health information obtained for underwriting activities may only be used or disclosed for that purpose.

A state entity that is an enforcement or oversight agency must require business associates, health care plans, or health care providers to comply with this policy.
[45 C.F.R. § 164.514(g)]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

State entities that are business associates, health care clearinghouses, health care plans, health care providers, or hybrid entities must implement policies and procedures to limit the health information disclosed to the amount reasonably necessary to achieve the purpose for the disclosure.
[45 C.F.R. § 164.514(d)(3)(i), and § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. At a minimum, state entities are responsible to do all of the following:
   1. Ensure that health information obtained during the underwriting process (including premium rating or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits) is not used for any other purpose if the patient's application for coverage is not approved.

2. The health plan may only use or disclose the obtained health information for the intended underwriting purpose, or as may be required by law.
3. Limit the use of health information, with respect to genetic information obtained for underwriting purposes, to determinations of health appropriateness or when a patient seeks a benefit.
4. State entities are prohibited from disclosing the health, medical, or genetic history of the patient to any financial or credit institution.
   [CA Civil Code § 56.265]
5. Any use or disclosure of information obtained during the underwriting process that is made on a routine and recurring basis, and which is allowed by state or federal law or regulations, must conform to the minimum necessary standards.
   [45 C.F.R. § 164.514(d)(3)(i)]

IV. References

45 C.F.R.

- § 164.514(d)(3)(i)
- § 164.514(g)
- § 164.530(i)(1)

CA Civil Code § 56.265

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Specially Protected Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.2.0 – Uses and Disclosures		
2.2.16 – Victims of Abuse, Neglect, or Domestic Violence		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the permitted uses and disclosures of health information for victims of abuse, neglect, or domestic violence.

II. Policy

Health information may be disclosed, without the patient's authorization, to a government authority authorized by law to receive reports when it is reasonably believed that the patient is the victim of abuse, neglect, or domestic violence.

Special restrictions on disclosures of information apply to the Department of State Hospitals and the Department of Developmental Services. These entities should consult with their legal counsel before disclosing health information or when developing and implementing operational policies and procedures.
[45 C.F.R. § 164.512(c); CA Civil Code § 56.10(c), § 56.104(e)(3), and § 1798.24; CA Health and Safety Code § 124250(a)(1)]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information related to victims of abuse, neglect, or domestic violence.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities may disclose health information, without a patient authorization, under any of the following circumstances:
   1. To the extent the disclosure is required by law

2. If the victim agrees to the disclosure
3. To the extent the disclosure is expressly authorized by law, *and* either of the following:
   a. When the state entity determines the disclosure is necessary to prevent serious harm to the patient or other potential victims
   b. The patient is unable to agree due to incapacity; *and both of the following are met:*
      i. A law enforcement or other public official, authorized to receive the report, represents that the health information is not intended to be used against the patient, and
      ii. The law enforcement or other public official, authorized to receive the report, represents that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.
4. To Disability Rights California, if the disclosure is necessary for Disability Rights California to exercise its authority to investigate incidents of abuse of neglect of people with disabilities (see *SHIPM Chapter 2, Developmental Services Records*). *Due to the complexity of state requirements related to Disability Rights California, state entities are advised to consult with their legal counsel prior to developing and applying operational policies and procedures governing the use and disclosure of health records.*
   [CA Civil Code § 1798.24b.(b)(4)(A); CA Welfare and Institutions Code § 4902(b)(1)]

B. State entities that make a disclosure permitted above must promptly inform the patient or the patient's representative that such a report has been or will be made, unless either of the following applies:
   1. The state entity determines that informing the patient would place the patient at risk of serious harm.
   2. The report would be made to the patient's representative, and the state entity determines the patient's representative may be responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient.

[45 C.F.R. § 164.512(c); CA Civil Code § 56.05(e), and § 56.104(e)(3); CA Health and Safety Code § 124250(a)(1); CA Welfare and Institutions Code §§ 5510(a)(1) – (3)]

C. State entities are responsible for documenting, tracking and accounting for all disclosures of health information involving victims of abuse, neglect or domestic violence. Documentation must be keep for a minimum of six (6) years *(see SHIPM Chapter 5, Accounting of Disclosures)*.

IV. References

45 C.F.R.

- § 164.512(c)
- § 164.530(i)(1)

CA Civil Code

- § 56.05(e)
- § 56.10(c)
- § 56.104(e)(3)
- § 1798.24

CA Health and Safety Code

- § 124250(a)(1)
- § 130303

CA Welfare and Institutions Code

- § 4902(b)(1)
- §§ 5510(a)(1) – (3)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 5 – Accounting of Disclosures

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2 – Uses and Disclosures		
2.2.17 – Health Information Exchange (HIE)		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: Yes

I. Purpose

To explain the permitted uses and disclosures of health information for health information exchange (HIE) purposes.

II. Policy

A valid written contract or other written agreement must be agreed to and implemented between organizations prior to using, disclosing, moving, or storing health information for health information exchange purposes.
[42 U.S.C. § 17901, and § 17938]

For uses and disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for HIE purposes.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Health information exchange is necessary and beneficial within a standardized framework that protects the privacy of health information and the security of data being exchanged.
[CA Civil Code § 56.10(a), and § 56.11]

B. A state entity that uses or discloses health information as part of a HIE, must comply with all SHIPM policies pertaining to specially protected health information, as well as its own policies and those of the California Office of Information Security (OIS).

C. If the state entity is engaging in health information exchange with:

1. One other organization. A state entity must enter into a written contract or other written agreement with the organization with which it intends to exchange information. *At a minimum*, the agreement must address all of the following:
   a. The minimum requirements of a valid business associate agreement (BAA) to fulfill all of the requirements and obligations of a business associate (BA) in regard to the privacy, security, and administrative activities relating to health information (see *SHIPM Chapter 4, Business Associate Agreement*)
      i. If the contracting entity and organization are *both* government entities, the entity can fulfill the agreement requirement with a memorandum of understanding that contains terms that accomplish the objectives of a BAA.
      [45 C.F.R. § 164.314(a)(2)(ii), and § 164.504(e)(3)(i)]
      ii. If the contracting entity is a group health plan and the organization is a plan sponsor, the written agreement must ensure the organization safeguards electronic health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan, and that the group health plan's plan documents address the same safeguards and protections for electronic health information as for any other health information shared with the sponsor.
      [45 C.F.R. § 164.314(b), and § 164.504(f)]
   b. The scope of the organization's services and functions
   c. The uses, disclosures, and any further disclosures of health information the organization is permitted or required to make when it has received the information
   d. The safeguards the organization will implement to protect the privacy and security of health information
      [42 U.S.C. § 17938; 45 C.F.R. § 164.308(b), and § 164.314(a)]
   e. If the organization is required by law to perform a function for or provide a service to the state entity, the entity may proceed to disclose electronic health information to the organization to the extent necessary to comply with the legal mandate without a written agreement, as long as the state entity attempts in good faith and documents its efforts to obtain assurances that the organization will protect and treat as confidential the information shared
      [42 U.S.C. § 17938; 45 C.F.R. § 164.314(a)(2)(ii)(B), and § 164.504(e)(3)(ii)]
2. A health information organization (HIO). The state entity must enter into a written contract or other written agreement with the HIO providing health information exchange oversight and services and the HIO's participating entities.

Examples of types of organizations that require such agreements include Regional Health Information Organizations, e-prescribing Gateways, and any vendor that contracts with a state entity to allow that state entity to offer personal health data to patients as part of its electronic health record.
[42 U.S.C. § 17938]

At a minimum, the agreement must address all of the following:

a. The minimum requirements of an adequate BAA
b. The scope of the HIO's governance, services and functions
c. The use, disclosure, and any further disclosure of health information the HIO and its participating entities are permitted or required to make as they create, receive, move, transmit, store, or maintain electronic health information
d. The safeguards the HIO and its participating entities will implement to protect the privacy and security of the electronic health information
[42 U.S.C. § 17938; 45 C.F.R. § 164.308(b), § 164.314(a), §§ 164.502(e)(1) – (2), and § 164.504(e)]
e. In the context of a networked HIO environment, the entity may enter into a single, multi-party BAA with multiple entities or organizations participating in the exchange of health information

3. An organization consisting of multiple HIOs. The state entity must enter into a written agreement with any HIOs providing health information exchange services along with their participating entities.
[42 U.S.C. § 17938]

At minimum, the agreement must address all the following:

a. The minimum requirements of an adequate BAA
b. The scope of the multi-HIO's governance, services, and functions
c. The use, disclosure, and further disclosures of health information the multi-HIO and its participating HIOs and entities are permitted or required to make as they create, receive, move, transmit, store, or maintain electronic health information
d. The safeguards the multi-HIO and its participating HIOs and entities will implement to protect the privacy and security of the electronic health information
[42 U.S.C. § 17938; 45 C.F.R. § 164.308(b), § 164.314(a), §§ 164.502(e)(1) – (2), and § 164.504(e)]
e. In the context of a networked multi-HIO environment, state entities are required to use the California Data Use and Reciprocal Support Agreement (CalDURSA) as its written agreement with the multi-HIO organization, or a written agreement with all the same elements as the CalDURSA (*see CalDURSA document*).

State entities participating in health information exchange with a single HIO are encouraged, but not required, to use the CalDURSA as its written agreement where applicable.

[45 C.F.R. § 164.308(b), and §§ 164.502(e)(1) – (2); CA Civil Code § 56.10(a), and § 56.37(a)]

IV. References

42 U.S.C.

- § 17901
- § 17938

45 C.F.R.

- § 164.308(b)
- §§ 164.314(a) – (b)
- §§ 164.502(e)(1) – (2)
- §§ 164.504(e) – (f)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(a)
- § 56.11
- § 56.37(a)

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 4 – Health Information Organizations
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

Yes - California Data Use and Reciprocal Support Agreement (CalDURSA), dated July 24, 2014

Chapter: 2 – Privacy		
Section: 2 – Uses and Disclosures		
2.2.18 – Hybrid Entities (MOVED to 4.6.5)		
Review Date: N/A	Revision Date: N/A	Attachments: No

This policy has been moved to Chapter 4 – Requirements for Specific Organizations – see 4.6.5 – Hybrid Entities.

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.1 – Genetic Information		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance regarding the use or disclosure of genetic information for underwriting purposes.

II. Policy

Except for a health care plan that is an issuer of a long-term care policy where the policy is not a nursing home fixed indemnity policy, genetic information shall not be used by health care plans for underwriting purposes.

Underwriting does not include determination of medical appropriateness when a patient is seeking a benefit under a health care plan, coverage, or policy.
[45 C.F.R. § 160.103, and § 164.502(a)(5)(i); CA Civil Code § 56.17; CA Health and Safety Code § 124980(j)]

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose genetic health information.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities that are health care plans, including hybrid entities that have a health care plan component, shall not collect or use genetic information to enroll individuals in a plan, or disclose genetic information to a third party administrator (TPA) or another state entity for underwriting purposes.

   Exception to the prohibition: Issuers of long-term care policies in which an employee welfare benefit plan provides health benefits to employees of two or more employers.

   Note: This is a discrete exception, which is unlikely to apply to many state entities.

B. State entities that are group health care plans and health insurance issuers may not adjust premiums or contribution amounts for a plan, or any group of similarly situated individuals under the plan, based on genetic information alone without manifestation of any disease or disorder of one or more individuals in the group.

IV. References

45 C.F.R.

- § 160.103
- § 164.502(a)(5)(i)
- § 164.530(i)(1)

CA Civil Code § 56.17

CA Health and Safety Code

- § 124980(j)
- § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Underwriting

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.2 – HIV/AIDS Information		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance on the uses and disclosures of human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome (AIDS) information.

II. Policy

Information about HIV or AIDS is a type of specially protected health information and must be protected, used, or disclosed *only* as allowed by law.
[CA Health and Safety Code § 120980, § 121025(a), and § 121065]

Due to the complexity and potential consequences related to HIV/AIDS information, state entities are encouraged to consult with their legal counsel prior to developing and applying operational policies and procedures governing the use and disclosure of HIV/AIDS information.

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose HIV/AIDS information and test results.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are responsible for doing all of the following:
   1. Know and comply with any state or federal restrictions on disclosures of HIV/AIDS information.
   2. State entities that are permitted by law to use and disclose HIV/AIDS information for public health or criminal investigative purposes are responsible to know and follow any specific departmental policies authorizing the use and disclosure.

B. With a patient authorization. State entities may use and disclose HIV/AIDS information as described in the written patient authorization.

Written authorization is required for each separate disclosure of HIV/AIDS test results, except for those disclosures that do not require an authorization, as described in *Section III.C - below*.
[CA Health and Safety Code § 120980(g)]

C. Without a patient authorization. State entities are permitted to disclose HIV/AIDS test results to any of the following:

1. To the patient or the patient's representative.
2. To the patient's health care provider who provides direct patient care and treatment.
3. Health care plans and insurance entities are not included in the SHIPM health care provider definition. So, disclosures to health care plans and insurance entities for this purpose are not permitted without a patient authorization.
4. To a health care provider who procures, processes, distributes, or uses a donated human body part.
5. To a designated officer of an emergency response organization regarding possible exposure to HIV or AIDS.

   However, the disclosure is only permitted to the extent necessary to comply with the provisions of the federal Ryan White Comprehensive AIDS Resources Emergency Act of 1990. *[Public Law 101-381; 42 U.S.C. § 201]*

[45 C.F.R. § 164.502(a)(1)(i); CA Health and Safety Code § 120985, and § 121010; CA Civil Code § 56.05(m)]

D. Minimum necessary. Disclosures must include only the information necessary for the purpose of that disclosure and the receiver must agree the information will be kept confidential and not further disclosed without a written authorization.
[45 C.F.R. § 164.502(b), and § 164.514(d); CA Health and Safety Code § 121025(c)]

E. Notice of Privacy Practices. State entities that disclose HIV/AIDS test results information must reference how this information will be used or disclosed, and provide an example in the Notice of Privacy Practices *(see SHIPM Chapter 5, Notice of Privacy Practices).*

IV. References

Public Law 101-381

42 U.S.C. § 201

45 C.F.R.

- §§ 164.502(a)(1)(i) – (a)(1)(ii)
- § 164.502(b)
- § 164.514(d)
- § 164.530(i)(1)
- § 164.530(j)

CA Civil Code § 56.05(m)

CA Health and Safety Code

- § 120980
- § 120985
- § 121010
- § 121025
- § 121065
- § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.3 – Mental Health Records		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance on the use and disclosure of mental health records to persons or entities other than the patient who is the subject of the record.

II. Policy

Mental health records are a type of specially protected health information and may only be used or disclosed as provided by law.

Psychotherapy Notes and Developmental Services Records are addressed in other SHIPM policies *(see SHIPM Chapter 2, Psychotherapy Notes; and Developmental Services Records*).

Due to the complexity of state requirements related to mental health records, state entities are encouraged to consult with their legal counsel prior to disclosing health information or developing and implementing operational policies and procedures governing the use and disclosure of mental health records.

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose mental health information.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. With an authorization. State entities may disclose mental health record information with an authorization from the patient or patient's representative,

   If the information is provided to a county mental health patients' rights advocate providing services, the patient or patient's representative may revoke the authorization at any time, verbally or in writing.
   [45 C.F.R. § 164.524(c)(3)(ii); CA Welfare and Institutions Code § 5328(a)(13), § 5541, and § 5542]

B. Without an authorization. Without an authorization from the patient or patient's representative, a state entity may disclose information from mental health records, but only the minimum necessary information, under the following circumstances:

1. To inform those involved in the patient's care or to inform the patient's attorney upon verification. Mental health record information may be disclosed without an authorization if, in the professional judgment of the mental health staff/provider, the patient lacks capacity and disclosure is in the best interest of the patient.
   [CA Civil Code § 56.104; CA Welfare and Institutions Code § 5328(a)(10)]
2. For coordination of a minor's care and custody. Mental health record information may be disclosed to a county social worker, a probation officer, or any other person who is legally authorized to have custody or care of a minor patient who has been taken into temporary custody, or is a dependent child or ward of the court or juvenile court, for the sole purpose of coordinating health care services and medical treatment, mental health services, or developmental services for the patient.
   [CA Welfare and Institutions Code § 5328.04]
3. To inform others of patient's admission to or presence in a treatment facility. If the patient is unable to authorize the release of information, only information confirming the patient's presence in a public or private treatment facility shall be provided upon request of a family member (spouse, parent, child, or sibling of a patient).
   [CA Welfare and Institutions Code § 5328.1(a)]
4. To inform others of patient activities in a 24-hour treatment facility. A 24-hour public or private health facility must make reasonable attempts to notify the patient's next of kin, or other person designated by the patient, of the patient's admission, unless the patient requests otherwise.
   [CA Welfare and Institutions Code § 5328.1]
5. In situations with risk of serious harm. A patient's psychotherapist who believes a patient presents a serious danger of violence may release mental health record information to potential victim(s), to law enforcement officials and county child welfare agencies if the psychotherapist determines the disclosure is needed to protect potential victims.
   [45 C.F.R. § 164.512(j); CA Welfare and Institutions Code § 5328(a)(18)]

6. To protect and advocate for disability rights. Mental health information and records must be disclosed to Disability Rights California under certain circumstances (see *SHIPM Chapter 2, Developmental Services Records*).

   Due to the complexity of state requirements related to Disability Rights California, state entities are advised to consult with their legal counsel prior to developing and applying operational policies and procedures governing the use and disclosure of mental health records.

   [CA Welfare and Institutions Code § 4902(b)(2)]

7. To determine or investigate conservatorships. Mental health information and records may be disclosed by treatment facilities to the courts conducting conservatorship procedures.

   [CA Welfare and Institutions Code § 5328(a)(6), and § 5354]

8. When a committed patient escapes. The medical director of the treatment facility may disclose the least amount of information considered essential to identify an escapee (e.g., patient's name, reason for commitment, age, physical condition) for a patient who was committed to a state mental health facility, after being found not guilty by reason of insanity, unable to stand trial, or is a mentally disordered sex offender.

   [45 C.F.R. § 164.512(j); CA Welfare and Institutions Code § 5328(a)(15), § 6250, § 7325, and § 7325.5; CA Penal Code § 290.004, § 1026, and § 1368]

9. To provide services inside the facility. Qualified professionals working in the same facility or having responsibility for the patient's care may share the patient's mental health record information to provide services or referral for services.

   [CA Welfare and Institutions Code § 5328(a)(1)]

10. In response to criminal activity while hospitalized. The director of the facility or designee may disclose mental health record information to law enforcement officials, when they believe a patient has committed, or has been the victim of, specified crimes (e.g., murder, manslaughter, mayhem, kidnapping, carjacking, robbery, arson, extortion, rape).

    The disclosure shall be limited to the minimum information necessary to investigate the crimes.

    [45 C.F.R. § 164.512(f); CA Welfare and Institutions Code § 5328.4]

11. In support of a claim for payment. Mental health record information necessary for the patient to make a claim for aid, insurance or medical assistance may be disclosed.

    [CA Welfare and Institutions Code § 5328(a)(3)]

12. For the administration of justice. Mental health record information may be or is required to be shared with the courts, as indicated below:
    a. When instructed through a court order – required
    b. When requested with a subpoena ordering delivery to the court - permitted as long as the patient has been given notice and an opportunity to object and other required conditions are met *(see SHIPM Chapter 2, Judicial and Administrative Proceedings)*
    c. For all other law enforcement or justice related requests (*see SHIPM Chapter 2, Law Enforcement)*

    [45 C.F.R. § 164.512(e), and § 164.512(f); CA Welfare and Institutions Code § 5328(a)(6), and § 5328.02]
13. To facilitate research. Mental health record information may be disclosed, as provided for in regulations adopted by the California Departments of Health Care Services, State Hospitals, Social Services or Developmental Services, specifying rules and necessary approvals for the conduct of research, and specifying confidentiality requirements for researchers.
    [CA Welfare and Institutions Code § 5328(a)(5), and § 5329]
14. For purposes of licensing inspections. Mental health record information may be disclosed to licensing personnel, consistent with the minimum necessary standard, to enable the performance of their duties to inspect, license and investigate health facility and community care facilities, under certain conditions.

    Due to the complexity of state requirements in this area, state entities are encouraged to consult with their legal counsel prior to developing and implementing operational policies and procedures governing the use and disclosure of mental health records for this purpose.
    [45 C.F.R. § 164.512(d); CA Welfare and Institutions Code § 5328.15(a)]
15. For purposes of quality assurance. Mental health record information may be disclosed to the California Department of Health Care Services for mental health quality assurance purposes.

    Due to the complexity of state requirements in this area, state entities are advised to consult with their legal counsel prior to developing and applying operational policies and procedures governing the use and disclosure of mental health records for this purpose.
    [45 C.F.R. § 164.512(d); CA Welfare and Institutions Code § 5328(a)(14), and § 14725]

16. When a patient dies. If a patient dies from any cause while hospitalized in a state mental hospital, information shall be released to a medical examiner, forensic pathologist, or coroner upon request.

    The information provided to the medical examiner, forensic pathologist, or coroner shall remain confidential and shall include only the information that may be disclosed pursuant to applicable federal and state law.
    [45 C.F.R. § 164.508(a)(2)(ii) and § 164.512(g)(1); CA Civil Code § 5610(b)(8) and § 56.11(c)(4); CA Welfare and Institutions Code § 5328.8]

IV. References

45 C.F.R.

- § 164.508(a)(2)(ii)
- §§ 164.512(d) – (g)
- § 164.512(j)
- § 164.524(c)(3)(ii)
- § 164.530(i)(1)

CA Civil Code

- § 56.10(b)(8)
- § 56.104
- § 56.11(c)(4)

CA Health and Safety Code § 130303

CA Penal Code

- § 290.004
- § 1026
- § 1368

CA Welfare and Institutions Code

- § 4902(b)(2)
- § 5328
- § 5329
- § 5354
- § 5541
- § 5542
- § 6250
- § 7325
- § 7325.5
- § 14725

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Judicial and Administrative Proceedings
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Specialized Government Functions
SHIPM Chapter 2 – Treatment, Payment, and Health Care Operations (TPO)
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Genetic Information
SHIPM Chapter 2 – Substance Use Disorder Treatment
SHIPM Chapter 2 – Developmental Services Records
SHIPM Chapter 2 – Psychotherapy Notes
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Patient's (Personal) Representative
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.4 – Substance Use Disorder Treatment		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance on the use and disclosure of a patient's substance use disorder treatment records, a subset of specially protected health information.

II. Policy

Substance use disorder treatment records are a type of specially protected health information and may only be used or disclosed as authorized by law or an authorization. *[42 U.S.C. § 290dd-2; 42 C.F.R. § 2.12(a)(1); 45 C.F.R. § 164.506; CA Health and Safety § 11845.5]*

Due to the complexity of federal and state laws related to substance use disorder treatment records, state entities involved in the use or disclosure of this information are encouraged to consult with their legal counsel prior to developing and implementing operational policies and procedures governing the use and disclosure of these records.

III. Implementation Specifics

Note that special restrictions in this policy apply only to substance use disorder treatment records.

A. State entities must have in place formal policies and procedures to reasonably protect against unauthorized use and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information. The policies and procedures must address:

   1. Paper records, to include:
      a. Transferring and removing records
      b. Destroying records, including sanitizing hard copy media associated with the paper printouts, to render the patient identifying information non-retrievable
      c. Maintaining records in secured rooms, locked file cabinets, safes, or other containers, or storage facilities when not in use
      d. Using and accessing workstations, secured rooms, locked containers, or storage facility that use or store records

e. Rendering patient identifying information non-identifiable in a manner that creates a very low risk of re-identification

2. Electronic records, to include:
   a. Creating, retrieving, maintaining, and transmitting records
   b. Destroying records, including sanitizing the electronic media on which records are stored, to render the patient identifying information non-retrievable
   c. Using and accessing electronic records and other electronic media containing patient identifying information
   d. Rendering patient identifying information non-identifiable in a manner that creates a very low risk of re-identification

   [42 C.F.R. § 2.16]

B. State entities may disclose substance use disorder treatment records for specific purposes when the patient or patient's representative provides written authorization *(see SHIPM Chapter 2, Authorizations).*

   There are additional requirements on authorizations for substance use disorder treatment records:

   1. The authorization can be revoked, in whole or part, verbally or in writing. A state entity may request but cannot require a revocation for substance use disorder treatment records to be in writing.
      [42 C.F.R. § 2.1, and § 2.14; CA Health and Safety Code § 11845.5(b), and § 11845.5(c)(4)]
   2. The written authorization for a disclosure of substance use disorder treatment records must specifically include:
      a. Name of the patient
      b. Identification of the program, entities, or person permitted to make the disclosure
      c. How much and what kind of information can be disclosed
      d. Identification of the persons or entities with a treating provider relationship with the patient, persons, or entities without a treating provider relationship with the patient to whom the disclosure is to be made
      e. Purpose of disclosure
      f. Statement that consent is subject to revocation at any time
      g. Date, event, or condition upon which consent will expire
      h. Signature of patient
      i. Date on which consent is signed

      [42 C.F.R. § 2.31(a)]

3. Each disclosure via an authorization must be accompanied by a notice prohibiting further disclosure. The following language **must** be used:

   "(1) This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§ 2.12(c)(5) and 2.65; or (2) 42 CFR part 2 prohibits unauthorized disclosure of these records."
   [42 C.F.R. § 2.32]

C. State entities may disclose substance use disorder treatment records - without an authorization in the following circumstances:

   1. Communication within a program, or with another entity. Health information may be used or disclosed between, and among personnel having a need for the information to diagnose, treat, or make a referral for treatment of substance use disorder, if the communications are:

      a. Within a program, or

      b. Between a program and an entity that has direct administrative control over the program.

      [42 C.F.R. § 2.12(c)(3), § 2.12(d)(2), § 2.33(b), and § 2.34; CA Health and Safety Code § 11845.5(c)(1)]

   2. Child Abuse Reporting. State entities may disclose information that identifies a patient as an individual with a substance use disorder to report suspected child abuse or neglect to appropriate state or local authorities. However, substance use disorder treatment records may not be disclosed for any follow-up inquiries or requests for information without an authorization or court order *(see SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence*).

      Note: Consult your legal counsel for the sufficiency of any court order.
      [42 C.F.R. § 2.12(c)(6)]

3. When needed for a qualified service organization to provide services to the program. State entities may disclose information needed by the qualified service organization to provide services to the organization.
   [42 C.F.R. § 2.11, § 2.12(c)(4), and § 2.12(d)(2); CA Health and Safety Code § 11845.5(c)(1)]
4. When needed to assist medical emergency personnel. Information may be disclosed about a patient for the purpose of treating a condition which poses an immediate threat to the health of *any* individual and which requires immediate medical intervention.
   [42 C.F.R. § 2.1, and § 2.51; CA Health and Safety Code § 11845.5(c)(2)]
5. When needed to report a patient's crimes or threatened crimes on program premises or against program personnel. Disclosures between program personnel and law enforcement officials are limited to circumstances of the incident, including the patient's name, address, and last known whereabouts without revealing that the person is a patient for treatment.
   [42 C.F.R. § 2.12(c)(5); CA Health and Safety Code § 11845.5(a) and (c)(5)]
6. When needed to conduct research, management or financial audits, or program evaluation. The records can be disclosed to *qualified personnel*, as long as any report on such activities does not identify patients in any way.

   Qualified personnel means persons whose training and experience are appropriate to the nature and level of work in which they are engaged, and who, when working as part of an organization, are performing that work with adequate administrative safeguards against unauthorized disclosures.
   [42 C.F.R. § 2.1, § 2.52, and § 2.53; CA Health and Safety Code § 11845.5(c)(3)]
7. When needed to comply with a sufficient court order. *State entities should consult with their legal counsel.*
   [42 C.F.R. § 2.1, and §§ 2.61 - 2.67; CA Health and Safety Code § 11845.5(c)(5)]

D. Additional requirements. State entities are responsible to know and comply with the following additional requirements on substance use disorder treatment records:

1. For deceased patients, disclosure of identifying information is permitted for the collection of death or other vital statistics, or to a coroner for resolving inquiries into the cause of death *(see SHIPM Chapter 2, Decedents*).

   Any other disclosure of specially protected health information identifying a deceased patient as an individual with a substance use disorder requires a patient's representative to provide authorization.
   [42 C.F.R. § 2.15(b)]

2. State entities are responsible for protecting the confidentiality of substance use disorder treatment records of an applicant to a program or any past or present patient.
   [42 C.F.R § 2.1; 42 U.S.C. § 290dd-2; CA Civil Code § 56.30(i); CA Health and Safety Code § 11845.5(a), and § 11845.5(e)]
3. State entities may not acknowledge the presence of a patient presently in or having completed a program without an authorization or court order. A state entity may acknowledge the presence of a patient presently in a program without an authorization only when the facility is not a publically identified substance use disorder treatment facility and the facility does not identify the patient as an individual with a substance use disorder.
   [42 C.F.R. § 2.1, § 2.13(c), and § 2.14; CA Health and Safety Code § 11845.5(b), and § 11845.5(c)(4)]
4. Disclosures for a patient referred by the criminal justice system. A program may disclose information about a patient to those persons within the criminal justice system who have made participation in the program a condition of the disposition of any criminal proceedings against the patient, or that patient's parole, or other release from custody, *if*:
   a. The disclosure of substance use disorder treatment information is made only to those individuals within the criminal justice system who have a need for the information in connection with their duty to monitor the patient's progress (e.g., a prosecuting attorney who is withholding charges against the patient, a court granting pretrial or post-trial release, probation or parole officers responsible for supervision of the patient), *and*
      [42 C.F.R. § 2.35(a)]
   b. The written authorization includes a statement that automatically revokes it after a specific amount of time or the occurrence of a specific event. The time or occurrence upon which consent becomes revocable may be no later than the final disposition of the conditional release or other action in connection with which consent was given, *and*
      [42 C.F.R. § 2.35(c)]
   c. The individual receiving the specially protected health information uses or re-discloses it only to carry out official duties with regard to the patient's conditional release or other purposes for which the consent was given.
      [42 C.F.R. § 2.35]

E. Substance use disorder treatment records from a program that discontinues operations, or is acquired by or merged with other entities, must destroy its records or purge patient-identifying information from records, *unless*:

1. The patient who is subject of the records gives written permission to the transfer of the record to the acquiring program, or to any other program designated in the permission, *or*
2. There is a retention period specified by law, which does not expire until after the discontinuation or acquisition of the program. In which case the records must be sealed in an envelope or other container and labeled as follows:

   "*Records of [insert name of program] required to be maintained under [insert citation to statute, regulation, court order or other legal authority requiring that records be kept] until a date not later than [insert appropriate date]"*

   The envelope or container must be held by a responsible person who must, as soon as *practicable* after the end of the retention period specified on the label, destroy the records.

[42 C.F.R. § 2.19]

F. Notices to patients are required by federal law at the time of admission or as soon thereafter as the patient is capable of rational communication. Each program shall:
   1. Communicate to the patient that federal law and regulations protect the confidentiality of substance use disorder patient records, and
   2. Provide to the patient a written summary of the federal law and regulations, with the specific details defined in the law. Required elements of the notice:
      a. A general description of the limited circumstances under which a program may acknowledge that an individual is present at a facility or disclose outside the program information identifying a patient as having or having had a substance use disorder
      b. A statement that violation of the federal law and regulations by a program is a crime and that suspected violations may be reported to appropriate authorities in accordance with federal regulations, along with contact information
      c. A statement that information related to a patient's commission of a crime on the premises of the program or against personnel of the program is not protected
      d. A statement that reports of suspected child abuse and neglect made under state law to appropriate state and local authorities are not protected
      e. A citation to the federal law and regulations

      [42 C.F.R. § 2.22]
   3. Provide the patient the program/organization's Notice of Privacy Practices.

G. Patients have the right to access their own substance use disorder treatment records *(see SHIPM Chapter 5, Patient's (Individual's) Rights to Access Health Information).* *[42 C.F.R. § 2.23]*

IV. References

42 U.S.C. §§ 290dd–2
42 C.F.R. §§ 2.1 – 2.67
45 C.F.R. § 164.506
CA Civil Code § 56.30(i)
CA Health and Safety Code § 11845.5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.5 – Developmental Services Records		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance on the use and disclosure of developmental services records to persons or entities other than the patient who is the subject of the record.

II. Policy

Developmental service records are a type of specially protected health information and may only be used or disclosed as provided by law.

Psychotherapy Notes or Mental Health Records are addressed in other related SHIPM policies *(see SHIPM Chapter 2, Psychotherapy Notes; and Mental Health Records*).

Due to the complexity of state requirements related to developmental service records, state entities are encouraged to consult with their legal counsel prior to disclosing health information or developing and applying operational policies and procedures governing the use and disclosure of developmental services records.

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose developmental service records.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Authorization special requirement. A new authorization for developmental service records related information must be obtained for each separate specific use.

B. With an authorization. State entities may disclose developmental service records and related information with an authorization from the patient if he or she has the capacity to give informed consent, or from the patient's representative.
[CA Welfare and Institutions Code § 4514(b), and § 4514(d)]

C. Without an authorization. Without an authorization, a state entity may disclose information from developmental service records, but only the minimum necessary information, under the following circumstances:

1. For intake, assessment, services, referrals, and treatment. Developmental service records information may be disclosed without an authorization between professional persons within a regional center, state developmental center, or a program that is part of a regional center or state developmental center for these purposes.
   [CA Welfare and Institutions Code § 4514(a)]
2. To inform the patient's attorney upon verification of representation. Developmental service records information may be disclosed without an authorization if the patient lacks capacity to sign an authorization.
   [CA Welfare and Institutions Code § 4514(j)]
3. In support of a claim or application for services. Developmental service records information necessary to make a claim or application for aid, insurance, government benefit or medical assistance on the patient's behalf may be disclosed.
   [CA Welfare and Institutions Code § 4514(c)]
4. To inform family members of patient status in a treatment facility. If the patient with developmental disabilities lacks the capacity to provide informed consent and the patient's representative is unable to authorize the release for any reason, upon request the patient's immediate family (spouse, parent, child, or sibling) may be notified of the patient's presence in, release from, or death while in a state hospital, community care or health facility.
   [CA Welfare and Institutions Code § 4514.5]
5. In situations of suspected abuse. In cases of suspected abuse, information and records shall be reported to an agency mandated to investigate abuse, and in response to a request from such an agency to investigate cases of suspected abuse.
   [45 C.F.R. § 164.512(b)(1)(ii), and § 164.512(c); CA Welfare and Institutions Code § 4514(r), § 5328.5, and § 15630; CA Penal Code § 11164]
6. To protect and advocate for disability rights. Developmental service records information must be disclosed to Disability Rights California under certain circumstances.

   Due to the complexity of state requirements related to Disability Rights California, state entities are encouraged to consult with their legal counsel prior to developing and applying internal policies and procedures governing the use and disclosure of developmental service records to Disability Rights California.
   [42 U.S.C. § 10801, § 10805(a)(4)(C), § 15001, and § 15043(a)(2)(I)(iii); CA Welfare and Institutions Code § 4514(v), §§ 4900 - 4906, and § 5328.06]

7. For the administration of justice. Developmental service records information may, or is required to, be shared with the courts, as indicated below:
   a. When instructed through a court order – *required*.
   b. When requested with a subpoena ordering delivery to the court - *permitted* as long as the patient has been given notice and an opportunity to object, or other required conditions are met *(see SHIPM Chapter 2, Judicial and Administrative Proceedings)*.
   c. For all other law enforcement or justice related requests *(see SHIPM Chapter 2, Law Enforcement)*.

   [45 C.F.R. § 164.512(e), and § 164.512(f); CA Welfare and Institutions Code § 4514(f), § 5328(a)(6), and § 5328.02]
8. If reported missing or lost while hospitalized. The director of the facility or designee may disclose developmental service records information to law enforcement officials, when they believe a patient is lost or missing.

   The disclosure shall be limited to the minimum information necessary to investigate the disappearance.

   [45 C.F.R. § 164.512(f); CA Welfare and Institutions Code § 4514(p)]
9. In response to criminal activity while hospitalized. The director of the facility or designee may disclose developmental service records information to law enforcement officials, when they believe a patient has committed, or has been the victim of, specified crimes (e.g., murder, manslaughter, mayhem, kidnapping, carjacking, robbery, arson, extortion, rape, etc.).

   The disclosure shall be limited to the minimum information necessary to investigate the crimes.

   [45 C.F.R. § 164.512(f); CA Welfare and Institutions Code § 4514(p)]
10. To facilitate research. Developmental service records information may be disclosed, as provided for in regulations adopted by the Director of California Department of Developmental Services, specifying rules and necessary approvals for the conduct of research, and specifying confidentiality requirements for researchers. These rules shall include that researchers sign and execute a Code of Confidentiality.

    [45 C.F.R. § 164.512(i); CA Welfare and Institutions Code § 4514(e)]
11. For purposes of licensing inspections and investigations. Developmental service records information may be disclosed to authorized representatives of the California Department of Public Health or Department of Social Services, as necessary, to enable the performance of their duties to inspect, license and investigate health facilities or community care facilities, under certain conditions.

Due to the complexity of state requirements in this area, state entities are encouraged to consult with their legal counsel prior to developing and implementing operational policies and procedures governing the use and disclosure of developmental services records for this purpose.
[45 C.F.R. § 164.512(d); CA Welfare and Institutions Code §§ 4514(n) – (o); CA Health and Safety Code § 1278, § 1293.2, § 1421, and § 1431]

12. For purposes of quality assurance. Developmental service records information may be disclosed to the California Department of Developmental Services for developmental services quality assurance purposes.

    Due to the complexity of state requirements in this area, state entities are encouraged to consult with their legal counsel prior to developing and implementing operational policies and procedures governing the use and disclosure of developmental services for this purpose.
    [45 C.F.R. § 164.512(d); CA Welfare and Institutions Code § 4514(a), § 4514 (o), and § 14725]

13. When a patient dies. If a patient dies from any cause while hospitalized in a state developmental center, information shall be released to a coroner, medical examiner, or forensic pathologist upon request.

    The information provided to the coroner, medical examiner, or forensic pathologist shall remain confidential and shall include only that information that may be disclosed pursuant to applicable federal and state laws.
    [45 C.F.R. § 164.508(a)(2)(ii) and § 164.512(g)(1); CA Civil Code § 56.10(b)(8) and § 56.11(c)(4); CA Welfare and Institutions Code § 4514(m)]

IV. References

42 U.S.C.

- § 10801
- § 10805 (a)(4)(C)
- § 15001
- § 15043

45 C.F.R.

- § 164.508(a)(2)(ii)
- § 164.512
- § 164.530(i)(1)

CA Civil Code

- § 56.10(b)(8)
- § 56.11(c)(4)

CA Health and Safety Code

- § 1278
- § 1293.2
- § 1421
- § 1431
- § 130303

CA Penal Code § 11164

CA Welfare and Institutions Code

- § 4514
- §§ 4900 – 4906
- § 5328
- § 5328.02
- § 5328.06
- § 5328.5
- § 14725
- § 15630

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Judicial and Administrative Proceedings
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Specialized Government Functions
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Genetic Information
SHIPM Chapter 2 – Mental Health Records
SHIPM Chapter 2 – Substance Use Disorder Treatment
SHIPM Chapter 2 – Psychotherapy Notes
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Patient's (Personal) Representative
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.3.0 – Specially Protected Information		
2.3.6 – Psychotherapy Notes		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance on the use and disclosure of psychotherapy notes to patients or others.

II. Policy

Psychotherapy notes are a type of specially protected health information and may only be used or disclosed as specifically provided by law.
[45 C.F.R. § 164.501, and § 164.508 (a)(2)]

Due to the complexity of state requirements in this area, and the specific conditions and limitations that apply, state entities involved in the use or disclosure of psychotherapy notes and related records are encouraged to consult with legal counsel prior to developing and implementing operational policies and procedures governing use and disclosure of these records.

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose psychotherapy notes.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Disclosure of psychotherapy notes to persons or entities other than the patient. State entities are responsible to obtain an authorization for any use or disclosure of psychotherapy notes to persons or entities other than the patient, *except when*:
   1. Needed to carry out treatment, payment or health care operations (TPO), only as described below (this use diverges from the health information TPO provisions):
      a. Only when used for treatment by the originator of the psychotherapy notes.
      b. Only when used or disclosed for an entity's own training programs in which mental health students, trainees, or practitioners under supervision practice or improve skills in group, joint, family, or individual counseling.

c. Only when used or disclosed by the entity to defend itself in a legal action or other proceeding brought by the patient who is the subject of the action.

Due to the complexity of laws and regulations regarding use or disclosure for legal action, state entities are encouraged to consult with their legal counsel prior to releasing information.

[45 C.F.R. § 164.508 (a)(2)(i); CA Welfare and Institutions Code § 5328.04(h)]

2. The use or disclosure is:

a. Required by the Secretary of U.S. Department of Health and Human Services as necessary to investigate or determine HIPAA compliance.
[45 C.F.R. § 164.502(a)(2)(ii)]

b. Required by a health oversight agency providing oversight of the originator of the psychotherapy notes.
[45 C.F.R. § 164.512(d)]

c. To a coroner, forensic pathologist, or medical examiner upon request for the limited purpose of identifying a deceased patient, determining a cause of death, or other duties as authorized by law.
[45 C.F.R. § 164.508(a)(2)(ii) and § 164.512(g)(1); CA Civil Code § 56.10(b)(8) and § 56.10(c)(4); CA Welfare and Institutions Code § 4514(m)]

d. Required by law. Provided that the use and disclosure is limited to the relevant requirements of such law for:

i. Disclosures about victims of abuse, neglect, or domestic violence to appropriate government authorities *(see SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence*)

ii. Disclosures for court orders
[45 C.F.R. § 164.512(a); CA Civil Code § 56.10(b), and § 56.10(c); CA Welfare and Institutions Code § 4514, and § 5328]

iii. When necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, ***and*** the disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat, *and* limited to a description of the perpetrator/escapee

[45 C.F.R. §164.501, and § 164.512(j)(1)(i); CA Welfare and Institutions Code § 5328(a)(18); CA Penal Code § 1328; Tarasoff v. Regents of the University of California – California Supreme Court decision]

B. Disclosure of psychotherapy notes to the patient. Regardless of a patient's (or patient representative's) authorization or request, a health care provider may decline to provide copies or permit inspection of the psychotherapy notes if the health care professional determines there is a substantial risk of significant adverse or detrimental consequences to a patient seeing or receiving copies of the notes or records *(see SHIPM Chapter 5, Patient's (Individual's) Rights to Access Health Information)*. *[CA Health and Safety Code § 123115(b)]*

IV. References

45 C.F.R.

- § 164.501
- § 164.502(a)(2)(ii)
- § 164.508 (a)(2)
- § 164.512(a)
- § 164.512(d)
- § 164.512(g)(1)
- § 164.512(j)(1)(i)
- § 164.530(i)(1)

CA Civil Code §§ 56.10(b) – (c)

CA Health and Safety Code

- § 123115(b)
- § 130303

CA Penal Code § 1328

CA Welfare and Institutions Code

- § 4514
- § 5328

Case Law - Tarasoff v. Regents of the University of California, 17 Cal. 3d 425, 551 P.2d 334, 131 Cal. Rptr. 14 (Cal. 1976)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Judicial and Administrative Proceedings
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Mental Health Records
SHIPM Chapter 2 – Psychotherapy Notes
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.4.0 – Breach and Breach Notification		
2.4.1 – Breach and Breach Notification		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: Yes

I. Purpose

To provide guidance regarding what must be done if a breach (unlawful or unauthorized access, acquisition, use or disclosure) of health information is thought to have occurred.

II. Policy

Breaches that compromise the security or privacy of patients' health information must be investigated and mitigated, by:

- Notifying affected patients
- Documenting corrective actions
- Providing reports to appropriate oversight entities

Note: Breach includes unencrypted health information and encrypted health information (where the encryption key or security credential is also obtained).
[42 U.S.C. § 17932; 45 C.F.R. §§ 164.400 – 164.414; CA Civil Code § 1798.29; CA Health and Safety Code § 1280.15; CA SAM § 5340.4; CA SIMM §§ 5340A – C]

III. Implementation Specifics

A. Policies and Procedures. Policies and procedures must be developed, implemented, and maintained, to ensure compliance with legal requirements regarding identifying, investigating and reporting breaches or unauthorized disclosures of health information.
[45 C.F.R. § 164.316, and § 164.530(i); CA SAM § 5340.3; CA SIMM § 5340-C]

B. A breach is presumed to have occurred unless the state entity can demonstrate there is a low probability, based on a breach investigation and risk assessment, the health information has been compromised (*see section III.C – below*). The following do not constitute a reportable breach:

1. Any unintentional acquisition, access, or use of health information by a workforce member, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure not permitted by the privacy rule.
2. Any inadvertent disclosure by a person who is authorized to access health information to another person authorized to access health information at the same

covered entity or business associate, and the health information received is not further used or disclosed in a manner not permitted by the privacy rule.

3. A disclosure of health information where a workforce member has a good faith belief the unauthorized recipient of the information would not reasonably be able to retain the health information.

[45 C.F.R. § 164,402(1), and § 164.402(2)]

C. Conduct a Breach Investigation. Following the discovery of a breach (or suspected breach) of health information, state entities are responsible for conducting and documenting the results of a breach investigation, including a risk assessment.

All the following factors should be included in the breach investigation and risk assessment:

1. The nature and extent of the health information involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person or entity who used the health information or to whom the disclosure was made.
3. Whether the health information was actually acquired or viewed.
4. The extent to which the risk to patient(s) has been mitigated.

[45 C.F.R. §§ 164.400 –164.414; CA Civil Code §§ 56.10 –56.16, and §§ 1798.24 – 1798.24(b); CA SAM § 5340.3]

D. Report the Breach. If it is determined that a breach of health information has/may have occurred, state entities and their business associates (BA) that own, license, or maintain state data (includes electronic, paper, or any other medium), must do all of the following (*that apply*):

1. To the Office of Information Security (OIS) and the California Highway Patrol (CHP) California Compliance and Security Incident Reporting System (Cal-CSIRS). Immediately report and notify the OIS and the CHP Computer Crimes Investigation Unit (CCIU) of the breach using the Cal-CSIRS.

   Each state entity's Information Security Officer (ISO) is responsible for notifying the proper authorities (s*ee SHIPM Chapter 3 – Incident Procedures*).

   [CA Civil Code § 1798.29; CA SIMM §§ 5340-A - C; CA Penal Code § 502]

2. To the California Department of Public Health (CDPH) Licensing and Certification Division. A state entity that is a clinic, health facility, home health agency, or hospice, licensed by CDPH must report a breach to CDPH no later than 15 business days after the breach has been detected.

   [CA Health and Safety Code § 1280.15(b)(1)]

3. To other owners/licensees of the health information. State entity BAs, or other contracted entities, must immediately notify the state entity (Covered Entity) when there has been a suspected breach of health information.
4. To the California Office of Health Information Integrity (CalOHII). In the event of a breach affecting more than 500 individuals, notify CalOHII at: OHIcomments@ohi.ca.gov.

   In addition to notifying CalOHII in the event of a breach affecting more than 500 individuals, state entities must submit an annual accounting of any PHI specific breaches and suspected breaches to CalOHII at the end of each calendar year (and when requested by CalOHII). *Please use the attachment SHIPM CalOHII Annual Breach Reporting Form to document any suspected or confirmed breaches with the steps taken to investigate and mitigate each event.*

E. Required Notifications. Following a breach of protected health information, state entities that are covered entities are required to provide the following notifications:

1. To the Secretary of the U.S. Department of Health and Human Services (HHS). In the event a breach of health information affects 500 or more individuals/patients, HHS shall be notified at the same time notice is made to the affected individuals, in the manner specified on the HHS website.

   If fewer than 500 individuals/patients are affected, the state entity will maintain a log of the breaches to be submitted annually to HHS no later than 60 days after the end of each calendar year, in the manner specified on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.
   [45 C.F.R. § 164.408]
2. To the affected patients. Notifications must be sent to each patient who has had, or is reasonably believed to have had, health information unlawfully or unauthorized accessed, acquired, used, or disclosed. *See sections below regarding required methods, content and timing of notifications.*
3. Record unauthorized disclosure in accounting log. All impermissible disclosures must be recorded in the state entity's Accounting of Disclosure tracking tool/log. The log must record, at a minimum, the date of disclosure, name and address of the entity who received the health information, a brief description of the information disclosed, and a brief description of the reason for the disclosure (*see SHIPM Chapter 5, Accounting of Disclosures*).
   [45 C.F.R. § 164.528]

4. During the creation of the breach notification to patients, state entities must do all of the following (*that apply*):
   a. Provide OIS with draft notice. Submit (using Cal-CSIRS) to the OIS a draft breach notice for review and approval prior to the release.
   [CA SIMM §§ 5340-B - C]
   b. Report to the California Attorney General's office. For any single breach that requires notification to more than 500 California residents, state entities shall electronically submit a single sample copy of the notification, excluding personally identifiable information, to the Attorney General.
   [CA Civil Code § 1798.29]
   c. Provide the media with a press-release. In the event the breach affects more than 500 California residents, prominent media outlets serving the state and regional area shall be notified without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.
   [45 C.F.R. § 164.406; CA SIMM § 5340-C]

F. Methods of patient notifications. The notification must be sent by first-class mail to the patient, at his or her last known address.
   1. If the patient agrees to an electronic notice, email notification is permitted.
   2. If the state entity believes there is possible imminent misuse of any health information, notification may be provided by telephone or other means, as appropriate.
   3. Deceased patients. If the state entity knows the patient is deceased and has the address of the next of kin or personal representative of the patient, notification by first-class mail to the next of kin or personal representative shall be carried out.
   4. Substitute notification methods. If there is insufficient or out-of-date contact information that prevents written notification to the patient, a substitute form of notice shall be provided as follows:
      a. To fewer than ten (10) patients, notice may be provided by an alternative form of written notice, by telephone, or by other means.
      b. To ten (10) or more patients, notice may be provided by either a conspicuous posting for a period of 90 days on the home page of the entity's website, or a conspicuous notice in major print or broadcast media in the entity's geographic areas where the patients affected by the breach likely reside.

   [45 C.F.R. § 164.404(d)(2); CA Civil Code § 1798.29(i)(3)]

G. Content of patient notifications. The notification shall be written in plain language and titled "Notice of Data Breach." The overall format of the notice shall call attention to the nature and significance of the information, titles and headings will be clear and conspicuously displayed as well the text of the notice will be no smaller than 10-point type. The notice shall include all of the following, to the extent possible, using the prescribed headings:

1. Using the title "What Happened" provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach. As well, include whether the notification was delayed as a result of a law enforcement investigation.
2. Using the title "What Information Was Involved" provide a description of the types of health information involved in the breach (e.g., full name, SSN, date of birth, etc.).
3. Using the title "What We Are Doing" provide a brief description of what the state entity is doing to investigate the breach, to mitigate harm to the patients, and to protect against further breaches.
4. Using the title "What You Can Do" provide advice on any steps individuals should take to protect themselves from potential harm resulting from the breach. Also, provide the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, driver's license, or California identification card number.
5. Using the title "Other Important Information" provide the enclosure "Breach Help – Consumer Tips from the California Attorney General." This information is available in English and in Spanish and can be downloaded from: http://www.privacy.ca.gov/consumers/index.shtml
6. Using the title "For More Information" provide the following statement "For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov."
7. Using the title "Agency Contact" provide the name of the designated agency official or agency unit handling inquiries along with a toll-free phone number and website.

[45 C.F.R. § 164.404(c)(1); CA Civil Code § 1798.29; CA SIMM § 5340-C]

H. Timing of notifications. Breach notifications shall be made in accordance with the following:

1. A state entity that is a clinic, health facility, home health agency, or hospice, licensed by the CDPH, must send a breach notification to the affected patient or patient's representative no later than 15 days after the breach has been detected.

a. A law enforcement agency may delay notification by a state entity that is a clinic, health facility, home health agency, or hospice no more than 60 days after a written request, or 30 days after an oral request is made by the law enforcement agency regarding a criminal investigation.

[CA Health and Safety Code § 1280.15]

2. All other state entities must send a breach notification within ten (10) business days from the date breach was determined, or reasonably believed to have occurred, to the extent possible. However, notification is required without unreasonable delay, and no later than 60 calendar days.
   a. Any decision to delay notification beyond ten (10) days, but less than 60 days, should be made by the state entity's Agency Head, in writing.
   b. Notification may be delayed if a law enforcement agency determines the notification will impede a criminal investigation.

   [45 C.F.R. § 164.404(a)(2)(b), and § 164.412; CA Civil Code § 1798.29; CA SIMM §5340-C]

I. Documentation retention. State entities are responsible to retain breach policies and procedures documentation, as well as documentation related to any breach investigations, including the risk assessment and results, notifications, and reports made, for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is later.

[45 C.F.R. § 164.414(b), and § 164.530(j)]

IV. References

42 U.S.C. § 17932

45 C.F.R.

- §§ 164.400 – 164.414
- § 164.528
- § 164.530(i)

CA Civil Code

- §§ 56.10 – 56.16
- §§ 1798.24 – 1798.29

CA Health and Safety Code § 1280.15

CA Penal Code § 502

CA SAM

- § 5340.3
- § 5340.4

CA SIMM §§ 5340-A – C

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 3 – Incident Procedures
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 3 – Security Awareness and Training
SHIPM Chapter 4 – Sanctions of Violation
SHIPM Chapter 4 – Trading Partner Agreements
SHIPM Chapter 4 – Business Associate Agreements
SHIPM Chapter 5 – Accounting of Disclosures

VI. Attachments

Yes – SHIPM CalOHII Annual Breach Reporting Form

Chapter: 2 – Privacy		
Section: 2.5.0 – De-identification		
2.5.1 – De-identification		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance regarding the two methods that can be used to satisfy the HIPAA Privacy Rule's de-identification standard: Expert Determination and Safe Harbor.

II. Policy

Health information that identifies, or can reasonably be used to identify a patient, shall not be disclosed unless the disclosure is in compliance with federal and state laws, or the health information has been appropriately de-identified.

State entities are responsible for understanding requirements for de-identifying health information so it is no longer individually identifiable health information.

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to de-identify health information.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. Through "Expert Determination". State entities may determine that health information is no longer individually identifiable when a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

1. Determines after applying principles and methods, that there is minimal risk the information could be used, alone or in combination with other reasonably available information, by a recipient to identify a patient.
2. Documents the methods and results of the analysis that justifies (or supports) the determination.
   Experts may be found in the statistical, mathematical, or other scientific domains. From an enforcement perspective, the relevant professional experience and academic or other training of the expert used by the covered entity, as well as

actual experience of the expert using health information de-identification methodologies would be reviewed.

3. Guidance of generally accepted statistical and scientific principles and methods may be found in:
   a. The Statistical Policy Working Paper 22 – Report on Statistical Disclosure Limitation Methodology (https://www.hhs.gov/sites/default/files/spwp22.pdf) originally prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget.
   b. The Checklist on Disclosure Potential of Proposed Data Releases (https://nces.ed.govFCSM/cdac_checklist.asp) prepared by the Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget.

[45 C.F.R. § 164.514(b)(1)]

B. "Safe Harbor" approach to de-identification. In order to de-identify health information, state entities must remove all the following identifiers of the patient or their relatives, employers, or household members:
   1. Names, including initials of the patients associated with the corresponding health information (i.e., the subjects of the records) and of their relatives, employers, and household members must be suppressed. There is no explicit requirement to remove the names of providers or workforce members of the covered entity or business associate.
   2. All geographic subdivisions smaller than a state, including:
      a. Street address
      b. City
      c. County
      d. Precinct
      e. Zip codes, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
         i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
         ii. The initial three digits of a restricted zip code for all such geographic units containing 20,000 or fewer people are changed to 000. State entities are expected to rely on the most current publicly available Bureau of Census data regarding zip codes. This information can be downloaded from,or

queried at, the American Fact Finder website (http://census.gov/data/what-is-data-census-gov.html).

3. All elements of dates (except year) directly related to a patient, including:
   a. Birth date
   b. Admission date
   c. Discharge date
   d. Date of death
   e. All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone and Fax numbers
5. Electronic mail addresses
6. Social Security Numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate or license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images
17. Any other unique identifying number, characteristic, or code, except as permitted by HIPAA

State entities may not release information if they know that the information can be used alone, or in combination with other information available to the intended recipient of the information, to identify a patient. The HHS Office for Civil Right's de-identification paper is available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[45 C.F.R. § 164.514(b)(2)]

C. Re-identification of information. State entities may assign a code or other means of record identification to allow information to be re-identified, if:

1. The code or other means of record identification is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient (such as when a derivative of the patient's name is used as the unique record identifier).
2. The state entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.
3. Generally, a code or other means of record identification that is derived from health information would have to be removed from data de-identified following the "safe harbor" method.

   The implementation specifications provide an exception with respect to re-identification by the state entity. 45 C.F.R. § 164.514(c) permits covered entities to assign certain types of codes or other record identification to the de-identified information so that it may be re-identified by the covered entity at some later date. Such codes or other means of record identification assigned by the covered entity are not considered direct identifiers that must be removed.

IV. References

45 C.F.R.

- §§ 164.514(a) – (c)
- § 164.530(i)(1)

CA Health and Safety Code § 130303

V. Related Policies

Chapter 1 – CalOHII Authority
Chapter 2 – Research

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.6.0 – Incidental Disclosures		
2.6.1 – Incidental Disclosures		
Review Date: 06/01/2019	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To provide guidance regarding incidental uses and disclosures of health information and required policies and procedures.

II. Policy

State entities must exercise due diligence to limit and prevent incidental disclosures.

III. Implementation Specifics

A. Policies and Procedures. State entities are responsible to develop and implement policies and procedures that require their workforce to limit and prevent disclosures of health information. When those disclosures are incidental to a permitted or required use or disclosure, it does not apply to *impermissible* uses or disclosures.
[45 C.F.R. § 164.530(i)]

Policies and procedures must address all of the following:

1. The minimum necessary requirement. Health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.
[45 C.F.R. § 164.502(b)]
2. The implementation specifications for the minimum necessary requirement. Policies and procedures must identify the persons or classes of persons within the state entity who need access to the information to carry out their job duties, the categories or types of health information needed, and conditions appropriate to such access.
[45 C.F.R. § 164.514(d)]
3. The requirement that a state entity has appropriate safeguards in place to protect the privacy of health information.
[45 C.F.R. § 164.530(c)]

B. Safeguards. State entities must limit and prevent, to the extent possible, incidental uses or disclosures made to an otherwise permitted or required use or disclosure.

Reasonable safeguards include all of the following:

1. Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area.
2. Avoiding using patient names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality.
3. Isolating or locking file cabinets or records rooms.
4. Using secure treatment screens in joint treatment areas.

C. Accounting of disclosures. A state entity is not required to include incidental disclosures in an accounting of disclosures *(see SHIPM Chapter 5, Accounting of Disclosures)*.

D. Notice of Privacy Practices. State entities must include language to address incidental disclosures in their Notice of Privacy Practices *(see SHIPM Chapter 5, Notice of Privacy Practices)*.

IV. References

45 C.F.R.

- § 164.502(b)
- § 164.514(d)
- § 164.530

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Physical Safeguards
SHIPM Chapter 4 – Policy and Procedures
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.7.0 – Minimum Necessary		
2.7.1 – Minimum Necessary		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance that health information requested, used, or disclosed, must be limited to only the minimum necessary required for the specific use, disclosure, or request.

II. Policy

When health information is requested, used, or disclosed, steps must be taken to limit the amount of health information only to that which is relevant and necessary to accomplish the intended purpose.
[45 C.F.R. § 164.502(b); CA Constitution, Article 1, § 1; CA Civil Code § 56.10, and § 1798; CA SAM § 5310, and § 5310.2]

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to limit disclosure of health information to the minimum necessary.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities are responsible to:

1. Limit the use and disclosure of health information to the minimum amount of information necessary to accomplish the intended purpose.
   [45 C.F.R. § 164.502(b)(1); CA Civil Code § 56.10, § 56.11, and § 1798.24]
2. When requesting health information from another entity, ask for only the information needed to accomplish the purpose.
   [CA Civil Code § 1798.14]
3. Exempt from the minimum necessary requirement. The minimum necessary requirement does not apply to the following:
   a. Disclosures to or requests by providers for treatment purposes.
   b. Disclosures made to the patient who is the subject of the record, when requested or required.
   c. Uses or disclosures made pursuant to a valid authorization.

d. Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rule.

e. Disclosures to the Secretary of the U.S. Department of Health and Human Services when disclosure of information is required under the Privacy Rule for enforcement purposes.

f. Uses or disclosures required by state or federal law.

[45 C.F.R. § 164.502(b)]

IV. References

45 C.F.R.

- § 164.502(b)
- § 164.530(i)(1)

CA Constitution, Article 1, § 1

CA Civil Code

- § 56.10
- § 56.11
- § 1798
- § 1798.14
- § 1798.24

CA Health and Safety Code § 130303

CA SAM

- § 5310
- § 5310.2

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Uses and Disclosures

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.8.0 – Patient's (Personal) Representative		
2.8.1 – Patient's (Personal) Representative		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance regarding the requirements to treat a patient's representative as the patient, with respect to the uses and disclosures of the patient's health information, as well as the patient's rights under the law.

II. Policy

Patient representatives are to be treated the same as the patient for purposes of authorizing the uses and disclosures, as well as access of health information, and for an accounting of disclosures of health information.
[45 C.F.R. §§ 164.502(g)(1) – (3)(i); CA Civil Code § 56.10, and § 1798.24(c); CA Health and Safety Code § 123100]

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information to a patient's representative.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. A patient's representative, except in the situations described under section *III.C Access to records - exceptions* below, has all of the rights of the patient for the purposes of authorizing uses and disclosures, accessing health information and receiving an accounting of disclosures.

B. A patient representative is someone who is:

1. The parent, legal guardian, or someone who has the legal right to make health care decisions for the patient.

   The legal right to act on behalf of the patient must be supported by documentation which includes a description of the representative's authority to act for the patient *(see SHIPM Chapter 2, Uses and Disclosures and Authorizations*).

[45 C.F.R. § 164.502(g)(3)(i), and § 164.508(b)(6)(vi); CA Welfare and Institutions Code § 5350, and § 5541; CA Health and Safety Code §§ 123105(e)(1) – (4), and § 123110]

2. The executor, administrator, or other person with the authority to act on behalf of a deceased patient or the deceased patient's estate.
   [45 C.F.R. §§ 164.404(d)(1)(ii) – (d)(2), § 164.502(g), and § 164.502(g)(4)]

C. Access to records - exceptions. An individual meeting the conditions of being a patient's representative for a living patient does ***NOT*** have to be treated as a patient by state entities under certain conditions.

It is state policy that a health care provider considering the facts and their patients' best interest, can decide to deny access to a patient's representative in the following scenarios:

1. The state entity has information and a reasonable belief that the patient has been or may be a victim of abuse, neglect, or domestic violence through the actions or inactions of the patient's representative *(see SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence)*.
   [45 C.F.R. § 164.502(g)(5)(i)(A), and § 164.512(c)(2)(ii)]
2. The state entity has information the patient may be endangered by extending patient's rights to the patient's representative
   [45 C.F.R. § 164.502(g)(5)(i)(B), and § 164.512(c)(2)(i)]
3. The state entity, in exercise of professional judgment, decides it is not in the patient's best interest to extend patient's rights to the patient's representative
   [45 C.F.R. § 164.502(g)(5)(ii), and § 164.512(c)(2)(ii)]
4. The patient is an unemancipated minor, and either of the following:
   a. The minor patient has the right to consent to a health care service and he or she has not requested another person be treated as the patient's representative.
      [45 C.F.R. § 164.502(g)(3)(i)(A)]
   b. The minor patient may lawfully obtain a health care service without the consent of the parent or guardian.
      [45 C.F.R. § 164.502(g)(3)(i)(B)]

Note: Failing to provide records to a patient's representative may result in a determination of unprofessional conduct under California law. Consult your organization's legal counsel before providing records.

D. State entities must verify the authority and identity of the person acting as the patient representative *(see SHIPM Chapter 3, Verification of Identity*).

E. Documentation. A state entity must retain any documentation, modifications or revocations related to a patient's representative for a minimum of six (6) years. *[45 C.F.R. § 164.508)(b)(6)]*

IV. References

45 C.F.R.

- §§ 164.404(d)(1) – (2)
- §§ 164.502(g)(1) – (5)(ii)
- § 164.508(b)(6)
- § 164.512(c)(2)
- § 164.530(i)(1)

CA Civil Code

- § 56.10
- § 1798.24(c)

CA Health and Safety Code

- § 123100
- §§ 123105(e)(1) – (4)
- § 123110
- § 130303

CA Welfare and Institutions Code

- § 5350
- § 5541

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Uses and Disclosures
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 4 – Administrative Requirements
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information

VI. Attachments

None

Chapter: 2 – Privacy		
Section: 2.9.0 – Requirements for Telehealth		
2.9.1 – Requirements for Telehealth		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: Yes

I. Purpose

To explain the privacy requirements related to telehealth activities.

II. Policy

Health care providers using telehealth to deliver health care services are responsible for implementing and maintaining security and privacy policies and procedures that address the unique circumstances involved in providing telehealth services.

III. Implementation Specifics

A. Policy and procedures. While not specifically required by law, because of the unique environment of providing telehealth services, policies and procedures are required by CalOHII for special adaptations including, but are not limited to:

1. Methods utilized for verifying the identities of the patient, the patient's representatives, if applicable, and health care providers at the beginning of each telehealth encounter
2. Updating risk analyses to include telehealth
3. Taking a more active compliance role in the coordination of telehealth services with outside organizations
4. Methods utilized for secure communication (e.g., do not use MS, Skype or Email for telehealth)
5. Methods utilized for monitoring communications containing electronic health information
6. Periodic review of telehealth processes and procedures to evaluate ongoing privacy and security of the technology

[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

B. Health care providers initiating the use of telehealth shall follow all requirements regarding the confidentiality and security of health information.
[45 C.F.R. § 160.103, and § 164.530; CA Business and Professions Code § 2290.5(b), § 2290.5(f), and § 2290.5(g); CA Health and Safety Code § 1348.8]

C. Documentation requirements. The following types of records related to telehealth services shall be kept for a minimum of six (6) years from the later of the creation of the document or the date the document was last in effect:

1. Policies and procedures, and changes to policies and procedures
2. Training offered, provided, and taken by workforce members
3. Risk Analyses conducted and the results and corrective actions to mitigate the risks

[45 C.F.R § 164.530; CA Business and Professions Code § 2290.5; CA Health and Safety Code § 1348.8, and § 1348.8(a)(7)]

IV. References

45 C.F.R.

- § 160.103
- § 164.530

CA Business and Professions Code

- § 2290.5
- § 2290.5(b)
- § 2290.5(f)
- § 2290.5(g)

CA Health and Safety Code

- § 1348.8
- § 1348.8(a)(7)
- § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 1 – Authorizations
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 3 – Security Awareness and Training

VI. Attachments

Yes – Telehealth Checklist

Chapter: 2 – Privacy		
Section: 2.10.0 – Multiple Covered Functions		
2.10.1 – Multiple Covered Functions		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To describe the permitted uses and disclosures of health information for organizations which perform multiple covered functions, such as those of a health care plan, health care provider, and/or health care clearinghouse.

II. Policy

Organizations which serve multiple functions may use or disclose health information only for the purpose related to the function being performed, and must segregate the information from any joint information systems.
[45 C.F.R. § 164.504(g)]

III. Implementation Specifics

While not specifically required by law, CalOHII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to ensure health information is appropriately used or disclosed in an organization with multiple functions.
[45 C.F.R. § 164.530(i)(1); CA Health and Safety Code § 130303]

Policies and procedures should address, but not be limited to, the following:

A. State entities which perform multiple functions must comply with all requirements of the types of functions performed within their organization. For example, if a state entity, within its organization, performs the functions of a health care plan and a health care provider, the entity would have to comply with the rules for both functions.

B. With the exception of the permitted sharing of health information for treatment, payment, or health care operation (TPO) purposes, state entities that perform multiple functions may disclose health information internally, without patient authorization, only for the purpose of the permitted function being performed.

C. State entities that serve multiple functions must segregate any patient information into separate systems, so that health information is not used or disclosed for a different purpose than that for which it was collected.

D. Some functions are common to multiple covered functions, such as TPO, and can be shared between functions.

However, health information that is not common to the purposes for which information was collected must be kept separate and not shared. For example, if a patient is only engaged with the organization's health care provider function, his or her health information cannot be shared internally to market the organization's health care plan function.

IV. References

45 C.F.R.

- § 164.504(g)
- § 164.530(i)(1)

CA Health and Safety Code § 130303

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Treatment, Payment, and Health Care Operations (TPO)

VI. Attachments

None

Chapter 3 – Security

Chapter: 3 – Security		
Section: 3.0 – Cross Reference		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: No

I. Purpose

To provide guidance on where to find specific HIPAA regulations within the SHIPM document.

The SHIPM Security chapter is driven by HIPAA regulations and provides the policy that must be followed to achieve HIPAA compliance. In developing the policies in this section, CalOHII reviewed only CA SAM § 5300 to ensure policy consistency. The specific SAM § 5300 reference is provided to assist the reader map to SAM for specific guidance on how to implement the policy specifics. SHIPM provides the overall policy but does not address how the policy is to be implemented.

The HIPAA Security regulations are not necessarily a one-to-one (e.g., Privacy, Patient Rights), and may be included in a SHIPM topic that has been:

- Combined with another security topic, or
- Renamed for reading ease

Administrative Safeguards	Specifics	45 C.F.R. § 164.308	Primary SHIPM Policy
Security Management Process	Risk Analysis	(a)(1)(ii)(A)	3.1.4 Security Management Process
	Risk Management	(a)(1)(ii)(B)	3.1.4 Security Management Process
	Sanction Policy	(a)(1)(ii)(C)	3.1.4 Security Management Process
	Information System Activity Review	(a)(1)(ii)(D)	3.1.4 Security Management Process
Assigned Security Responsibility	Assigned Security Responsibility	(a)(2)	SHIPM Chapter 4 – Administrative 4.1.4 Staffing: Privacy Official, Security Official
Workforce Security	Authorization and/or Supervision	(a)(3)(ii)(A)	3.2.4 Workstation Use and Security
	Workforce Clearance Procedure	(a)(3)(ii)(B)	3.2.4 Workstation Use and Security
	Termination Procedures	(a)(3)(ii)(C)	3.2.4 Workstation Use and Security

Administrative Safeguards	Specifics	45 C.F.R. § 164.308	Primary SHIPM Policy
Information Access Management	Isolating Health Care Clearinghouse Function	(a)(4)(ii)(A)	3.1.3 Information Access Management
	Access Authorization	(a)(4)(ii)(B)	3.1.3 Information Access Management
	Access Establishment and Modification	(a)(4)(ii)(C)	3.1.3 Information Access Management
Security Awareness and Training	Security Reminders	(a)(5)(ii)(A)	3.1.5 Security Awareness and Training
	Protection from Malicious Software	(a)(5)(ii)(B)	3.1.5 Security Awareness and Training
	Log-in Monitoring	(a)(5)(ii)(C)	3.1.5 Security Awareness and Training
	Password Management	(a)(5)(ii)(D)	3.1.5 Security Awareness and Training
Security Incident Procedures	Response and Reporting	(a)(6)(ii)	3.1.2 Incident Procedures
Contingency Plan	Data Backup Plan	(a)(7)(ii)(A)	3.1.1 Contingency Plan
	Disaster Recovery Plan	(a)(7)(ii)(B)	3.1.1 Contingency Plan
	Emergency Mode Operation Plan	(a)(7)(ii)(C)	3.1.1 Contingency Plan
	Testing and Revision Procedures	(a)(7)(ii)(D)	3.1.1 Contingency Plan
	Applications and Data Criticality Analysis	(a)(7)(ii)(E)	3.1.1 Contingency Plan
Evaluation	Evaluation	(a)(8)	3.1.6 Security Evaluations
Business Associate Contracts	Written contract or other arrangement	(b)(3)	SHIPM Chapter 4 – Administrative 4.4.1 Business Associates Agreement
Physical Safeguards	**Specifics**	**45 C.F.R. § 164.310**	**Primary SHIPM Policy**
Facility Access Controls	Contingency Operations	(a)(2)(i)	3.2.3 Facility Access Controls
	Facility Security Plan	(a)(2)(ii)	3.2.3 Facility Access Controls
	Access Control and Validation Procedures	(a)(2)(ii)	3.2.3 Facility Access Controls
	Maintenance Records	(a)(2)(iv)	3.2.3 Facility Access Controls
Workstation Use	Workstation Use	(b)	3.2.4 Workstation Use and Security
Workstation Security	Workstation Security	(c)	3.2.4 Workstation Use and Security

Physical Safeguards	Specifics	45 C.F.R. § 164.310	Primary SHIPM Policy
Device and Media Controls	Disposal	(d)(2)(i)	3.2.2 Device and Media Controls
	Media Re-use	(d)(2)(ii)	3.2.2 Device and Media Controls
	Accountability	(d)(2)(iii)	3.2.2 Device and Media Controls
	Data Backup and Storage (during transfer)	(d)(2)(ivi)	3.2.2 Device and Media Controls
Technical Safeguards	**Specifics**	**45 C.F.R. § 164.312**	**Primary SHIPM Policy**
Access Control	Unique User Identification	(a)(2)(i)	3.3.5 Access Control
	Emergency Access Procedure	(a)(2)(ii)	3.3.5 Access Control
	Automatic Logoff	(a)(2)(iii)	3.3.5 Access Control
	Encryption and Decryption (including data at rest)	(a)(2)(iv)	3.3.2 Encryption
Audit Controls	Audit Controls	(b)	3.3.1 Audit Controls
Integrity and Implementation Process	Mechanism to authenticate ePHI	(c)(2)	3.3.4 Integrity
Person or Entity Authentication	Person or Entity Authentication	(d)	3.1.7 Verification of Identity
Transmission Security	Integrity Controls	(e)(1)(i)	3.3.4 Integrity
	Encryption (FTP and email over internet)	(e)(1)(ii)	3.3.2 Encryption

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.1 – Contingency Plans		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance for contingency planning in the event an emergency or other occurrence damaging systems containing health information.

II. Policy

Policies and procedures must be implemented specifying how to respond to an emergency, or other unexpected occurrences (e.g., fires, natural disasters, system failures), that may damage systems containing health information.
[45 C.F.R. § 164.308(a)(7); CA Health and Safety Code §§ 123149 – 123149.5]

III. Implementation Specifics

A. At a minimum, state entities are responsible to develop and implement policies and procedures that contain the following (with regard to health information and contingency plans):

1. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Technology Recovery Plan (also referred to as disaster recovery plan) and Business Continuity Plan (also referred to as emergency mode operations plan) in the event of an emergency.
   [45 C.F.R. §164.310(a)(2)(i)]
2. Procedures to create and maintain retrievable exact copies of electronic health information (data backup plan).
   [45 C.F.R. § 164.308(a)(7)(ii)(A)]
3. Procedures to restore any loss of this information (Technology Recovery Plan).
   [45 C.F.R. § 164.308(a)(7)(ii)(B)]
4. Procedures to continue critical business practices for protection of this information while operating in an emergency mode (Business Continuity Plan).
   [45 C.F.R. § 164.308(a)(7)(ii)(C)]
5. Procedures for periodic testing and revision of contingency plans (testing and revision procedures).
   [45 C.F.R. § 164.308(a)(7)(ii)(D)]

B. Technical Mechanisms.

1. Each state entity shall identify and document all business functions and critical infrastructure.
2. Each state entity shall conduct a business impact assessment to identify:
   a. Critical functions and systems, and prioritize them based on necessity;
   b. Threats and vulnerabilities; and
   c. Preventive controls and countermeasures to reduce the state entity's risk level.

   [CA SAM § 5325]
3. Each state entity shall develop Business Continuity Plan(s) to include procedures for how the state entity will stay functional in a disastrous state.
   [CA SAM § 5325]
4. Each state entity shall conduct an assessment of the importance of specific applications and data, in support of the various contingency plan components (applications and data criticality analysis), including all of the following:
   a. Identifying the steps to safeguarding the state entity's electronic systems and electronic health information.
   b. Identifying the state entity's most vulnerable points with regard to electronic systems and electronic health information.
   c. Identifying the state entity's biggest threats to electronic systems and electronic health information.
   d. Identifying the steps, in priority order, for the state entity to achieve recovery of electronic systems, electronic health information, and business operations in the event of an emergency.

   [45 C.F.R. § 164.308(a)(7)(ii)(E)]
5. Each state entity shall develop a Technology Recovery Plan (TRP) in support of the state entity's Business Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster.
   a. Each state entity must keep its TRP up to date and provide annual documentation for those updates to the Office of Information Security (OIS).

   [CA SAM § 5325.1, § 5325.3, § 5325.4, and § 5325.5; CA SIMM § 5325-A]

C. Safeguards.

1. Each state entity shall conduct regular training to prepare individuals on their expected tasks.
   [CA SAM § 5325, and § 5325.2]

2. Each state entity shall conduct regular tests and exercises to identify any deficiencies and further refine the plans.
   [CA SAM § 5325, and § 5325.3]
3. Each state entity shall develop steps to ensure the Business Continuity Plan is maintained, and updated regularly.
   [CA SAM § 5325, and § 5325.1]
4. Each state entity shall establish an alternative storage site.
   [CA SAM § 5325.4]
5. Each state entity shall ensure they have alternate telecommunications services including necessary agreements to permit the resumption of information asset operations.
   [CA SAM § 5325.5]
6. Each state entity shall perform regularly scheduled backups of system and user-level information.
   [CA SAM § 5325.6]

IV. References

45 C.F.R.

- §164.308(a)(7)
- §164.310(a)(2)(i)

CA Health and Safety Code §§ 123149 – 123149.5

CA SAM §§ 5325 – 5325.6

CA SIMM § 5325-A

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Incident Procedures
SHIPM Chapter 3 – Security Management Process

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.2 – Incident Procedures		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To explain the requirements to establish guidelines (development and implementation of policies and procedures) for the identification, response, reporting, assessment, analysis, and the follow-up to information security incidents.

II. Policy

As part of an overall security incident and response program, policies and procedures must be implemented that describe how workforce members are to identify, report, respond, and mitigate security incidents affecting health information, as well as support the implementation of the incident response plan.

Note: The initial assessment of the incident will lead to the determination of whether the incident should be elevated to the level of a breach (see SHIPM Chapter 2, Breach and Breach Notification for more information). If the incident proves to be a breach of health information*, affecting 500 or more individuals, notify the California Office of Health Information Integrity (CalOHII) at ohicomments@ohi.ca.gov, concurrently with other required breach reporting.*

[45 C.F.R. § 164.304, §§ 164.308(a)(6)(i) – (ii), §§ 164.314(a)(2)(i)(C) – (b)(2)(iv), and §§ 164.316(a) – (b)(2)(iii); CA SAM §§ 5340 – 5340.4; NIST SP 800-53 Rev. 5 (family: Incident Response), and NIST SP 800-61 Rev. 2]

III. Implementation Specifics

A. State entities are responsible for implementing security incident response policies and procedures for all workforce members that:

1. Define what a security incident is for the state entity's business functions
2. List the possible types of security incidents and the required response for each type
3. Identify who the security incident must be reported to within the state entity *[CA SAM §5340.1]*

B. Additional policies and procedures are required to assist those workforce members responsible for the state entity's security incident response efforts, including, but not limited to, all of the following:

1. Identify and respond to a suspected or known security incident.
   a. Procedures to capture and log the incident. At a minimum, incident log information should include:
      i. Contact information for the person reporting the incident (to include name, email address and phone number)
      ii. Description of incident
      iii. Date, time and location of the incident
      iv. Date, time and how the incident was discovered
      v. Evidence of the incident
      vi. Make/model of the affected computer(s)
      vii. Internet Protocol (IP) addresses of the affected computer(s)
      viii. Assigned name of the affected computer(s)
      ix. Operating system of the affected computer(s)
      x. Location of the affected computer(s)
      xi. Actions taken to mitigate

      [CA SIMM § 5340-A]

   b. Procedures for Security Reporting. Implement procedures to ensure immediate reporting to California Compliance and Security Incident Reporting System (Cal-CSIRS) in accordance with State Information Management Manual (SIMM) criteria and procedures.
      [CA SAM § 5330.2, and §5340; CA SIMM § 5340-A, and § 5340-C]

   c. Procedures for processing Business Associate (BA) reported incidents/breaches. Implement procedures to receive, process and respond (if needed) to BA reported incidents and breaches.
      [45 C.F.R. § 164.314(a)(2)(i)(C)]

2. Mitigate, to the extent reasonable, the situation that caused the security incident. Consult with system owners to quarantine the incident and limit damage.
   [CA SAM § 5340]
3. Document the security incident, how the state entity responded, and the results (outcomes). These procedures should include, but not limited to:
   a. Incident Response Team. How the security incident is assigned, managed and investigated, along with the procedures for escalation, and internal reporting and response.
      [CA SAM § 5340; CA SIMM § 5340-C]

b. Procedure for notifying individuals. How to manage security incidents involving breach of personal information, especially health information (*see SHIPM* Chapter *2, Breach and Breach Notification*).
[CA Civil Code § 1798.29; CA SAM § 5340; CA SIMM § 5340-A, and § 5340-C]

c. Mobilizing emergency and third party investigation and response (if necessary).
[CA SAM § 5340]

d. Consulting with personnel management/human resources (HR), if there is a violation of appropriate use policy by workforce member(s).
[CA SAM § 5340]

e. Communicating with law enforcement, when actual or suspected criminal activity is involved.
[CA SAM § 5340]

f. Handling of the incident that includes preparation, detection, analysis, containment, eradication, and recovery as well as coordinating with business continuity planning activities.
[CA SAM § 5340.3]

4. Evaluate security incidents as part of the state entity's ongoing risk management activities.
[45 C.F.R. § 164.308(a)(6)]

C. State entities are responsible to test their incident response capability to determine its effectiveness, document the results, and incorporate lessons learned to continually improve the incident response plan and procedures.
[CA SAM § 5340.2, and § 5340.3]

D. State entities are responsible to train their workforce members on the organization's implemented security incident and response policies and procedures (*see SHIPM Chapter 3, Security Training and Awareness*).
[45 C.F.R. § 164.316(a)(2)(ii); CA SAM 5340.1]

E. Covered entities should also report serious cyber incidents to:

1. FBI Field Office Cyber Task Force – to find your local field office, refer to the FBI Field Office website.
2. U.S. Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) – email them at hc3@hhs.gov.
3. United States Computer Emergency Readiness Team (US-CERT) any suspicious activity, including cybersecurity incidents, cyber threat indicators and defensive measures, phishing incidents, malware, and software vulnerabilities.

[NIST SP 800-61 Rev. 2; HHS, Health Industry Cybersecurity Practices, Dec. 2018]

F. Documentation Retention. State entities are responsible to retain incident documentation for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is greater. This includes:

1. Incident policies and procedures documentation, and
2. Documentation related to security incidents (to include all work papers, notes, incident response forms, meeting minutes and other items relevant to the incident investigation).

[45 C.F.R. §§ 164.316(b)(2)(i) – (b)(2)(iii)]

IV. References

45 C.F.R.

- § 164.304
- § 164.308(a)(6)
- §§ 164.314(a)(2)(i)(C) - 164.314(b)(2)(iv)
- §§ 164.316(a) – (b)(2)(iii)

CA Civil Code § 1798.29

CA SAM

- § 5330.2
- §§ 5340 – 5340.4

CA SIMM

- § 5340-A
- § 5340-C

NIST

- SP 800-53 Rev. 5
- SP 800-61 Rev. 2

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 3 – Contingency Plans
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 3 – Security Awareness and Training

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.3 – Information Access Management		
Review Date: 06/01/2017	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To provide guidance on authority to access and restriction of access to health information, and explain the limits and conditions on workforce access.

II. Policy

Information access management policies and procedures must be developed, implemented and maintained, that specify *who* (persons or software programs) has access to *what* specific health information and under what conditions.

Following an organization's risk analysis, authority to access health information must be:

- Limited to instances where access is specifically permitted or required by law
- Limited to the minimum necessary information required to accomplish the intended purpose, as defined in the state entity's policies and procedures (including definition of what information can be accessed by classes of workforce or specific programs)
- Consistent with legal requirements on use and disclosure

[45 C.F.R. § 164.308(a)(4); CA Civil Code § 56.10, and § 1798.24 - § 1798.24(b); CA Health and Safety Code § 123149(g), and § 1280.18; CA SAM § 5315.6, and § 5360]

III. Implementation Specifics

A. State entities are responsible for establishing, and implementing information access management program policies and procedures, which must address the following:

1. Isolating health care clearinghouse functions. If a state entity is a health care clearinghouse, or a hybrid entity, that is part of a larger organization, the clearinghouse or health care component of its organization, must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
   [45 C.F.R. § 164.308(a)(4)(ii)(A)]

2. Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
   [45 C.F.R. § 164.308(a)(4)(ii)(B); CA SAM § 5315.6, and § 5360]
3. Access establishment and modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Include naming someone or a program that has responsibility for reviewing and authorizing access.
   [45 C.F.R. § 164.308(a)(4)(ii)(C); CA SAM § 5315.6, and § 5360]

B. State entities information access management safeguards must include:
   1. Periodic review of whether access or the extent of access is necessary (role-based access)
   2. Procedures for gaining access when it is appropriate, but the workforce is not usually granted access (e.g., when an attorney has access to an electronic health record)
   3. What triggers a review of whether, and what type of access is necessary (e.g., workforce transfer or a project ends)
   4. Assigning responsibility, someone or a program, for reviewing and authorizing access
   5. Document:
      a. Which workforce members can have access
      b. A list of workforce members who have access
      c. What levels of access does the workforce member have
      d. What the triggering events are for termination, beginning or change of access
   6. Identification of the types of access (e.g., such as to facilities and/or systems)
   7. Isolation of functions under specific conditions (e.g., health care clearinghouse or hybrid entity) to protect health information from unauthorized access
   8. How a user's access to health information is established, documented, reviewed, and modified by workstations, transactions, programs or processes

   [CA SAM § 5315.6, and § 5360]

IV. References

45 C.F.R. § 164.308(a)(4)

CA Civil Code

- § 56.10
- §§ 1798.24 –1798.24(b)

CA Health and Safety Code

- § 1280.18
- § 123149
- § 123149(g)

CA SAM

- § 5315.6
- § 5360

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 2 – Uses and Disclosures
SHIPM Chapter 3 – Access Control
SHIPM Chapter 3 – Workstation Use and Security
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 4 – Policies and Procedures

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.4 – Security Management Process		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding the requirements to conduct risk analysis and other risk management activities to prevent, detect, contain, and correct security violations related to the protection of health information.

II. Policy

Health information must be protected through the implementation of policies, and administrative processes and procedures that address all of the following:

- Periodic risk analyses (every two [2] years)
- Implementation of risk management activities
- A workforce member sanction policy
- Regular review of information system activity (such as review of audit logs and incident tracking reports)
- Documentation of measures

[45 C.F.R. § 164.306(e), §§ 164.308(a)(1), and § 164.316(b)(2)(iii); CA Government Code § 11549.3; CA SAM § 5305.7; NIST SP 800-30 Rev. 1, SP 800-39, and SP 800-53 Rev. 5]

III. Implementation Specifics

A. For all information systems that contain health information, state entities are responsible to have entity-wide policies and procedures for risk management that include all of the following:

1. Risk analysis/assessment. The first step is to identify and evaluate risks and vulnerabilities to health information in the state entities environment(s).

   State entities are responsible to define the processes, and to conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and the availability of health information held by their organization. The analysis should include identifying where all health information is located, and who has a need to access it (as well as who currently has access to it).

Note: Periodic risk analysis includes evaluating the organization at the:

a. Organizational level,
b. Mission/Business Process level, and
c. Information Asset level.

[45 C.F.R. § 164.308(a)(1)(ii)(A); CA SAM § 5305.6; NIST SP 800-30 Rev. 1]

2. Implement security measures sufficient to reduce risk and vulnerabilities to health information (to ensure the confidentiality, integrity and availability of the information) to a reasonable and appropriate level (risk management program).
   [45 C.F.R. § 164.308(a)(1)(ii)(B); CA SAM § 5305.7; CA SIMM § 5305-A; NIST SP 800-53 Rev. 5]
3. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the state entity *(see SHIPM Chapter 4, Sanctions for Violation*).
   [45 C.F.R. § 164.308(a)(1)(ii)(C)]
4. Regular review of information system activity (such as review of audit logs and incident tracking reports, and the sharing of threat information with the CA Department of Technology via direct electronic means) *(see SHIPM Chapter 3, Audit Controls*).
   [45 C.F.R. § 164.308(a)(1)(ii)(D); CA SAM § 5315, and § 5335.2]
5. Update appropriate documentation (including training) as policies and procedures change, or are retired.
   [45 C.F.R. § 164.306(e), §§164.308(a)(1)(i) – (a)(1)(ii), and §164.316(b)(2)(iii); CA Government Code §11549.3; NIST SP 800-30 Rev. 1, SP 800-39, and SP 800-53 Rev. 5]
6. Protect against reasonably anticipated threats or hazards. *[CA SAM § 5305.6(2)]*
7. Protect against any reasonably anticipated unlawful uses or disclosures.
   [CA SAM § 5305.6(2)(b)]

[CA SAM § 5305.2, § 5305.6, and § 5315.1]

B. The risk analysis/assessment process must include (at a minimum) the following:
   1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
      [CA SAM § 5305.7(1)]
   2. Identification of the state entity information assets that are at risk, with particular emphasis on the applications of information technology that are critical to state entity program operations. Identification of the threats to which the information assets could be exposed.
      [CA SAM § 5305.7(2)]

3. Assessment of the vulnerabilities, e.g., the points where information assets lack sufficient protection from identified threats.
   [CA SAM § 5305.7(3)]
4. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
   [CA SAM § 5305.7(4)]
5. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
   [CA SAM § 5305.7(5)]
6. Selection of cost-effective security management measures to be implemented.
   [CA SAM § 5305.7(6)]
7. Preparation of a report, to be submitted to the state entity head and to be kept on file within the state entity, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity.
   [CA SAM § 5305.7(7)]

[CA SAM § 5305.7 and § 5315.1]

Note: Recommended best practice risk analysis/assessment steps include the following:

1. *Determine frequency and triggers for risk assessments. (i.e. yearly or if new system or updates to systems are implemented)*
2. *Identify the scope of the analysis*
3. *Gather data*
4. *Identify and document potential threats and vulnerabilities*
5. *Assess current security measures*
6. *Determine the likelihood of threat occurrence*
7. *Determine the potential impact of threat occurrence*
8. *Determine the level of risk*
9. *Identify security measures and finalize documentation*

C. **ADDITIONAL STATE ENTITIES REQUIREMENTS**

1. State entities are responsible to develop, implement, and maintain a state entity-wide Information Security Program Plan (ISPP), to provide for the proper use and protection of its information assets. State entities must ensure:

a. The ISPP is approved, and disseminated by the state entity head responsible and accountable for risks incurred to the state entity's mission, functions, assets, image and reputation

b. The ISPP has identified the roles and responsibilities, and assigned management responsibilities for information security program management consistent with the roles and responsibilities described in CA SIMM 5305-A (*see SHIPM Chapter 4, Staffing: Privacy Official, Security Official*)

[CA SAM § 5305.1; CA SIMM § 5305-A]

2. State entities are responsible to establish and maintain an inventory of all of its information assets, including information systems, information system components, and information repositories (both electronic and paper). The inventory shall contain:

   a. A listing of all programs and information systems identified as collecting, using, maintaining, or sharing state entity information

   b. A categorization and classification of the information assets by program management, and based on the CA SIMM § 5305-A, and FIPS Publication 199

   The categorization and classification of information assets shall be utilized in the determination of an asset's needed level of protection.
   [CA SAM § 5305.5; CA SIMM § 5305-A; FIPS Publication 199]

3. State entities are responsible to manage their information assets using a documented System Development Life Cycle (SDLC) methodology that:

   a. Incorporates information security requirements and considerations

   b. Defines and documents operational information security roles and responsibilities throughout the information asset lifecycle

   c. Identifies individuals having information security roles and responsibilities (*see SHIPM Chapter 4, Staffing: Privacy Official, Security Official*)

   d. Integrates the organizational information security risk management process into the development lifecycle activities

   [CA SAM § 5315, § 5315.2, and § 5315.4; NIST SP 800-53 Rev. 5]

4. State entities are responsible to employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code.
   [CA SAM § 5355.1]

5. State entities are responsible to establish and document their security authorization method, authorizing the operation of information assets, and explicit acceptance of risks based on implementation of agreed-upon information security measures.
   [CA SAM § 4800, and § 5315.9]

6. State entities may receive information asset alerts, advisories, and directives from legitimate external sources and shall act on them. State entities are responsible to generate internal security alerts, advisories, and directories as necessary to mitigate state entity risk.
   [CA SAM § 5355.2]
7. State entities are responsible to conduct a security assessment. NOTE: this assessment or any penetration/vulnerability testing conducted by CA Military Department only partially meets the risk assessment requirements per HIPAA.
   [CA Government Code § 11549.3]
8. State entities are responsible to conduct a Privacy Threshold Assessment (PTA) and if necessary, a Privacy Impact Assessment (PIA) when the collection, use, maintenance, storage, sharing, disclosure or disposal of personal information is involved. The PTA and PIA shall be performed upon the development or procurement of new information systems, and when proposing changes to an existing system or processes.
   [CA SAM § 5310.8; CA SIMM 5310-C]

IV. References

45 C.F.R.

- § 164.306(e)
- § 164.308(a)(1)
- §§ 164.316(b)(2) – (iii)

CA Government Code § 11549.3

CA SAM

- § 4800
- § 5305.1
- § 5305.2
- § 5305.5
- § 5305.6
- § 5305.7
- § 5310.8
- § 5315
- § 5315.1
- § 5315.2
- § 5315.4

- § 5315.9
- § 5335.2
- § 5355.1
- § 5355.2

CA SIMM

- § 5305-A
- § 5310-C

FIPS Publication 199

NIST

- SP 800-30 Rev. 1
- SP 800-39
- SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Access Control
SHIPM Chapter 4 – Sanctions for Violation
SHIPM Chapter 4 – Staffing: Privacy Official, Security Official
SHIPM Chapter 4 – Consequences of Non-Compliance

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.5 – Security Awareness and Training		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: No

I. Purpose

To provide guidance regarding requirements to promote security awareness by providing mandatory training on how to protect health information to all workforce members, including management.

II. Policy

Reasonable and appropriate administrative safeguards must be implemented to protect health information, including promoting security awareness, and providing mandatory training to all workforce members regarding the organization's implemented security policies and procedures, so they know how to protect health information.
[45 C.F.R. § 164.308(a)(5), § 164.530(b)(1), and §§ 164.530(j)(1) – (2); CA SAM § 5320, and § 5355.2]

III. Implementation Specifics

A. State entities are responsible to ensure all workforce members, before accessing health information, are given security training regarding the organization's security policies and procedures.

At a minimum, this security awareness and training should reflect the organization's security policies and procedures about all the following topics:

1. Security reminders. Periodic security updates to remind workforce members of their role in protecting health information (e.g., discussion topics at monthly meetings, focused reminders posted in affected areas).
[45 C.F.R. § 164.308(a)(5)(ii)(A)]
2. Protection from malicious software. How to guard against, detect, and report malicious software (e.g., unauthorized downloads from the Internet, opening email attachments from unknown senders).
[45 C.F.R. § 164.308(a)(5)(ii)(B)]
3. Log-in monitoring. The procedures for monitoring log-in attempts and reporting discrepancies. The purpose is to make workforce members aware of log-in attempts that are not appropriate. *[45 C.F.R. § 164.308(a)(5)(ii)(C)]*

4. Password management. The procedures for creating, changing, and safeguarding passwords (e.g., prevent the sharing of passwords, not leaving written passwords in areas that are visible or accessible to others).
   [45 C.F.R. § 164.308(a)(5)(ii)(D)]

B. Periodic security retraining for ongoing awareness, based on operational changes, technology updates, and security risks should be conducted as needed and at least annually. *[CA SAM § 5320.1]*

C. Documentation requirements. State entities are required to document all of the following:
   1. Security awareness and training. Workforce member names and dates of training.
   2. Security reminders. State entities are responsible to document the security reminders they implement. Documentation should include the type of reminder, its message and the date it was implemented.
   3. Retention. A state entity must retain the security awareness and training documentation for six (6) years from the date of its creation, or the date when it last was in effect, whichever is later.

[45 C.F.R. §§ 164.530(j)(1) – (2); CA SAM 5320.3]

IV. References

45 C.F.R.

- § 164.308(a)(5)
- § 164.530(b)(1)
- §§ 164.530(j)(1) – (2)

CA SAM

- § 5320
- § 5320.1
- § 5320.3
- § 5355.2

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 3 – Security Awareness and Training
SHIPM Chapter 3 – Workforce Security

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.6 – Security Evaluations		
Review Date: 06/01/2017	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To provide guidance regarding the legal requirements for conducting and documenting technical and non-technical evaluations of security measures implemented to protect health information.

II. Policy

Security evaluations must be conducted periodically, to review measures implemented to protect health information (paper and electronic), or when either of the following occurs:

- Weaknesses are identified
- There are environmental or operational changes which may affect the security of health information

[45 C.F.R. § 164.306(e), § 164.308(a)(8), and § 164.316(b)(2)(iii); CA Health and Safety Code § 1280.18; CA SAM § 5330.1]

III. Implementation Specifics

A. Security evaluations must be performed to determine whether the implemented security controls continue to ensure the confidentiality, integrity, and availability of health information. Security evaluations must cover both technical (e.g., systems, hardware, workstations, mobile devices) and non-technical (e.g., physical and administrative) areas, including:

1. Legal, policy, standards, and procedure compliance review,
2. Vulnerability scanning, and
3. Penetration testing.

Note: It is recommended that security evaluations be conducted no less frequently than every two (2) years.
[45 C.F.R. § 164.308(a)(8); CA SAM § 5330.1]

B. Establish outcome-based metrics to measure the effectiveness and efficiency of the implemented security program and deployed security controls.
[CA SAM § 5305.9]

C. State entities are responsible to review and modify their implemented policies and procedures, whenever the following occurs:
   1. Security weaknesses are identified through required security evaluations, or
   2. In response to environmental or operational changes.

   [45 C.F.R. § 164.306(e), and § 164.316(b)(2)(iii)]

D. Documentation regarding security evaluations, and corrective actions, must be retained in writing for a minimum of six (6) years from the date of its creation, or the date it was last in effect, whichever is later.

   [45 C.F.R. §164.316(b)(2)(i)]

IV. References

45 C.F.R.

- § 164.306(e)
- § 164.308(a)(8)
- § 164.316(b)(2)(i)
- § 164.316(b)(2)(iii)

CA Health and Safety Code § 1280.18

CA SAM

- § 5330.1
- § 5305.9

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Security

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.7 – Verification of Identity (Person or Entity Authentication)		
Review Date: 06/01/2017	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To explain the process and documentation required to verify a requestor's identity and authority prior to the disclosure of health information.

II. Policy

Policies and procedures must be implemented and maintained which specify that prior to disclosing health information, the identity of the requestor must be verified, and the authority that entitles the requestor to access health information must be established.
[45 C.F.R. § 164.312(d), and § 164.514(h)]

III. Implementation Specifics

A. State entities are responsible for establishing and implementing policies and procedures to verify the identity and authority of a person, or entity requesting access to health information prior to disclosing health information.
[45 C.F.R. § 164.514(h)]

B. Prior to disclosing health information to someone other than, or claiming to be the patient, state entities are responsible to obtain documentation to verify the *identity* and the *authority* of the requesting party if the identity or any such authority of such person is not known to the covered entity.

This includes, but is not limited to, requests:

1. Made in person (non-public official, or non-law enforcement)
2. By mail or electronic mail
3. From third-party(s) (e.g., attorney, family member, friend of the patient)
4. From law enforcement
5. On behalf of a minor or dependent adult
6. By a health care provider or health plan

[45 C.F.R. § 164.514(h)(1)(i) – (ii); CA Civil Code § 1798.34; CA Health and Safety Code § 123110]

C. Verify the identity and authority of the person requesting the health information based on the purpose of the request, if the identity and authority is not already known.

The verification requirements are satisfied if the state entity relies on the exercise of professional judgment in making a use or disclosure, or acts on a good faith belief in making a disclosure.
[45 C.F.R. §§ 164.514(h)(1) - (2)(iv)]

1. Verification of *identify* for public officials. The following may be relied on to verify the *identity* of public officials:
   a. For in-person requests, presentation of an agency identification badge, other official credentials, or proof of government status
   b. Requests made on official public letterhead, when the requests are made in writing

   Consult with your entity's legal counsel if a request is received from persons acting on behalf of the public official, a written statement on appropriate government letterhead that the person is acting under the government's authority, or other evidence or documentation that establishes that the person is acting on behalf of the public official, such as a contract for services, memorandum of understanding, or purchase order.
2. Verification of *authority* for public officials. A written statement of the legal authority under which the information is being requested may be relied on to determine the *authority* of public officials to access health information.

   Consult with your entity's legal counsel if the request is made as a result of a legal process, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.
   [45 C.F.R. §§ 164.514(h)(1) – (2)(iv)]

IV. References

45 C.F.R.

- § 164.312(d)
- § 164.514(h)

CA Civil Code § 1798.34

CA Health and Safety Code § 123110

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Opportunity to Agree or Object
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Research

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.1.0 – Administrative Safeguards		
3.1.8 – Workforce Security (RETIRED June 2017)		
Review Date: N/A	Revision Date: N/A	Attachments: No

This policy was retired during the June 2017 SHIPM Update. This policy overlapped with content and requirements in 3.2.4 Workstation Use and Security.

HIPAA requirements from this policy are now addressed in 3.2.4 Workstation Use and Security.

Chapter: 3 – Security		
Section: 3.2.0 – Physical Safeguards		
3.2.1 – Access Control (MOVED to 3.3.5)		
Review Date: N/A	Revision Date: N/A	Attachments: No

This policy has been moved to the Technical Safeguards section – see 3.3.5 Access Control.

Chapter: 3 – Security		
Section: 3.2.0 – Physical Safeguards		
3.2.2 – Device and Media Controls		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide information regarding the security of devices and media within the entity/organization to safeguard and protect health information against unauthorized access, use, disclosure, alteration or modification when the device or media is destroyed or re-used.

II. Policy

Policies and procedures must be implemented to govern the receipt, re-use, and removal of devices and media that contain health information, into and out of an entity/organization, and the movement of these items within the entity/organization.

Polices regarding the use, access and audit controls of devices – such as laptops, mobile devices – are addressed in other SHIPM policies (*see SHIPM Chapter 3 – Workstation Use and Security; Access Control; and Audit Controls*).

Note: Non-electronic forms of media that contain health information are also covered by this policy (e.g., hardcopy paper).
[45 C.F.R. §§ 164.306(a)(1) – (3), § 164.310(d)(1), and § 164.530(c); CA SAM § 5365.2]

III. Implementation Specifics

State entities are responsible to safeguard devices and media that contain health information and ensure they are properly controlled when being stored, moved, decommissioned or destroyed.

The devices and media may include, but are not limited to, laptops, workstations, hard drives, magnetic tapes or disks, USB drives, mobile devices, copy machines/photocopiers, and other types of portable storage devices.
[45 C.F.R. §§ 164.306(d)(1) – (3); CA SAM § 5365.2; CA Government Code § 11549.3; NIST SP 800-53 Rev. 5, and SP 800-88 Rev. 1]

A. State entities are responsible to implement policies and procedures to control and protect health information when discarding or reusing devices or media. These policies and procedures must address all of the following:

1. Disposal. Implement policies and procedures to address the final disposition of health information and the devices or media on which it is stored. The devices or media must be sanitized and/or destroyed to ensure the data cannot be re-constructed and the health information or media is rendered unusable or inaccessible.
   [45 C.F.R. § 164.310(d)(2)(i); CA SAM § 5310.6, and § 5365.3; NIST SP 800-53 Rev. 5, and SP 800-88 Rev. 1]
2. Media re-use. Implement procedures to remove health information from media before the media is available for re-use. Regardless of the final intended destination, internal or external to the organization, the media must not contain residual representation of any data that would allow re-construction.
   [45 C.F.R. § 164.310(d)(2)(ii); CA SAM § 5365.3; NIST SP 800-88 Rev. 1]
3. Data backup and storage. Implement procedures to create retrievable, exact copies of health information, when needed, prior to moving devices or media (*see SHIPM Chapter 3, Contingency Plan*). *[45 C.F.R. § 164.310(d)(2)(iv)]*

B. State entities are responsible to implement technical mechanisms that ensure devices and media are adequately controlled prior to discarding or re-using. Examples of technical mechanisms include:
   1. Clearing. Sanitizing the device or media by applying logical techniques to remove data from all user-addressable storage locations, such as rewriting with new values or resetting to a factory state.
      [CA SAM § 5365.3; NIST SP 800-88 Rev. 1]
   2. Destruction. Sanitizing the device or media that results in the inability to further use for storage of data, such as pulverization or incineration.
      [CA SAM § 5365.3; NIST SP 800-53 Rev. 5, and SP 800-88 Rev. 1]
   3. Purging. Sanitizing the device or media by applying physical or logical mechanisms to render data recovery infeasible, such as using an appropriate rated degausser on a hard disk.
      [CA SAM § 5365.3; NIST SP 800-53 Rev. 5, and SP 800-88 Rev. 1]

C. Additional Safeguards.
   1. Accountability. Maintain documentation that records the movement of devices and electronic media that contain health information within the organization. The workforce member responsible for the devices or media should also be tracked.
      [45 C.F.R. § 164.310(d)(2)(iii)]
   2. Training. Train workforce members on, and to follow, the disposal and re-use policies and procedures as necessary and appropriate for their role and responsibilities.
      [45 C.F.R. § 164.306(a)(4), § 164.308(a)(5), and § 164.530(b)]

3. Destruction of data backup. Securely destroy any data backups when the moving of devices or media is completed and the data is no longer necessary. *[CA SAM § 5310.6, § 5325.6]*

D. Documentation Retention. State entities are responsible to retain policy and procedure documentation related to device and media controls, as well as any action, activity or assessment that is required to be documented by HIPAA, for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is greater. *[45 C.F.R. §§ 164.316(b)(1) – (2)]*

IV. References

45 C.F.R.

- §§ 164.306(a)(1) – (3)
- § 164.308(a)(5)
- §§ 164.310(d)(1) – (3)
- §§ 164.316(b)(1) – (3)
- §§ 164.530(b) – (c)

CA Government Code § 11549.3

CA SAM

- § 5310.6
- § 5325.6
- § 5365.2
- § 5365.3

NIST

- SP 800-53 Rev. 5
- SP 800-88 Rev. 1

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Contingency Plan
SHIPM Chapter 3 – Workstation Use and Security
SHIPM Chapter 3 – Audit Controls
SHIPM Chapter 3 – Access Control

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.2.0 – Physical Safeguards		
3.2.3 – Facility Access Controls		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide information regarding the physical security and protection of facilities and information systems to safeguard health information against unauthorized access, use, disclosure, disruption or modification.

II. Policy

Policies and procedures must be implemented to limit physical access to a state entities electronic information systems, used to store and process health information, and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
[45 C.F.R. §§ 164.310(a)(1) – (2); CA SAM § 5365, and § 5365.1; NIST SP 800-53 Rev. 5]

III. Implementation Specifics

A. State entities are responsible to develop, implement and maintain policies and procedures to properly authenticate and authorize access to its information systems or equipment, and the facility or facilities in which they are housed. The facility access control policies and procedures should, at a minimum, address the following:

1. Contingency operations procedures that allow authorized workforce access to facilities in support of restoration of lost data under the Technology Recovery Plan and Business Continuity Plan in the event of an emergency. The procedures should include the security measures while the contingency plans are active.
[45 C.F.R. § 164.308(a)(7)(i), and § 164.310(a)(2)(i); CA SAM § 5365; NIST SP 800-53 Rev. 5]
2. Facility security plan that safeguards facilities and equipment from unauthorized physical access, tampering, damage and theft. The organization should include information from their risk assessment to determine the authorized workforce to access facilities and equipment that contain health information.
[45 C.F.R. § 164.310(a)(2)(ii); CA SAM § 5365, and § 5365.1; NIST SP 800-53 Rev. 5]
3. Access control and validation procedures that control and validate a person's access to facilities based on their role or function, including visitor authentication

and control. The procedures should identify workforce members, roles or job functions authorized to access information systems and software programs for purpose of testing and revision.
[45 C.F.R. § 164.310(a)(2)(iii); CA SAM § 5315.4, and § 5365; NIST SP 800-53 Rev. 5]

4. Maintenance records that document repairs and modification to the physical components of a facility that are related to security.
[45 C.F.R. § 164.310(a)(2)(iv); NIST SP 800-53 Rev. 5]

[45 C.F.R. §§ 164.310(a)(1) – (a)(2); CA SAM § 5365; CA Government Code § 11549.3; NIST SP 800-53 Rev. 5]

B. State entities are responsible to implement technical mechanisms that ensure facilities are adequately controlled to protect health information. Examples of mechanisms include:

1. Documenting the types of locations that require access controls to safeguard health information (e.g., data centers, peripheral equipment centers, IT staff offices, workstation locations).
[NIST SP 800-53 Rev. 5]

2. Implementing physical access controls to restrict access at worksites both during and after work hours.
[CA SAM § 5365; NIST SP 800-53 Rev. 5]

3. Documenting the issuance of authorization credentials (such as access cards) for the facility where health information systems reside. Maintain a current list of workforce members with authorized access, and perform regular reviews and approval of the list.
[45 C.F.R. § 164.306(e); CA SAM § 5365; NIST SP 800-53 Rev. 5]

4. Implementing procedures to address continued maintenance of security (access control) during a service disruption of the secure access control (card) system, requiring alternate security measures.
[45 C.F.R. § 164.308(a)(7)(i), and § 164.310(a)(2)(i); CA SAM § 5365; NIST SP 800-53 Rev. 5]

5. Documenting the periodic change of access controls following security events (e.g., when keys are lost, combinations compromised, or individuals are transferred or terminated).
[CA SAM § 5365; NIST SP 800-53 Rev. 5]

C. Safeguards.

1. Train workforce members on implemented facility access controls policies and procedures, as necessary and appropriate for their role and responsibilities.
   [45 C.F.R. § 164.306(a)(4), § 164.308(a)(5), and § 164.530(b)]
2. Limit visitor access by protecting health information from unauthorized access, including incidental contact by visitors.
   [45 C.F.R. § 164.306(a)(3), and § 164.530(c)(2)(i) - (ii); NIST SP 800-53 Rev. 5]
3. Complete regular assessments of physical security to identify and correct vulnerabilities.
   [45 C.F.R. § 164.306(a)(2); NIST SP 800-53 Rev. 5]

D. Documentation Retention. State entities are responsible to retain policy and procedure documentation related to facility access controls, as well as any action, activity or assessment that is required to be documented by HIPAA, for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is greater.
[45 C.F.R. §§ 164.316(b)(1) – (2)]

IV. References

45 C.F.R.

- §§ 164.306(a)(2) - (4)
- § 164.306(e)
- § 164.308(a)(5)
- § 164.308(a)(7)(i)
- §§ 164.310(a)(1) - (2)
- §§ 164.316(b)(1) – (2)
- § 164.530(b)
- § 164.530(c)(2)

CA Government Code § 11549.3

CA SAM

- § 5315.4
- § 5365

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Contingency Plans
SHIPM Chapter 4 – Administration
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.2.0 – Physical Safeguards		
3.2.4 – Workstation Use and Security		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To outline the security requirements for all workstations, including mobile devices, that process, store, and transport/transmit health information**.**

II. Policy

Administrative, physical and technical safeguards must be implemented for all workstations, including mobile devices, that access health information in order to restrict access to individuals with authorization.
[45 C.F.R § 164.310, and § 164.310(b); CA Health and Safety Code § 1280.18; CA SAM § 5360.1, and § 5360.2]

III. Implementation Specifics

A. State entities are responsible to implement workstation and mobile device security policies and procedures to specify the proper functions to perform, the manner in which they are performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access health information.

In addition, the policies and procedures should protect health information from unauthorized access.
[45 C.F.R §§ 164.310(b) – (c); CA SAM § 5315]

B. State entities are responsible to implement the following administrative, physical, and technical safeguards to protect workstations and mobile devices.

1. Administrative safeguards.

   a. Procedures to regularly review system activity such as audit logs and system access reports.
   [45 C.F.R. § 164.308(a)(1)(ii)(D), and § 164.312(b); CA SAM § 5335, and § 5335.2]

   b. Procedures for the authorization and supervision of workforce members who work with health information.
   [45 C.F.R. § 164.308(a)(3)(ii)(A); CA SAM § 5305.4]

c. Policies and procedures to determine and allow appropriate access levels to health information for its workforce members (including remote and wireless access).
[45 C.F.R. § 164.308(a)(3)(ii)(B), and §§ 164.308(a)(4)(ii)(B) – (C); CA SAM § 5305.4, § 5305.5, § 5315.6, and § 5360]

d. Procedures for terminating access to health information when employment of a workforce member ends or as workforce members change assignments.
[45 C.F.R. § 164.308(a)(3)(ii)(C); CA SAM § 5305.4, § 5305.5, and § 5315.7]

e. Training of workforce on procedures to protect against malicious software, monitor login attempts, and manage passwords.
[45 C.F.R. §§ 164.308(a)(5)(ii)(B) – (D); CA SAM § 5355, and § 5355.1]

2. Physical safeguards.

a. Implementing physical security and environmental protection policies, procedures and controls, to guard against unauthorized access, use, disclosure, disruption, modification, or destruction of health information.
[45 C.F.R. § 164.310(a)(2)(ii); CA SAM § 5365; NIST SP 800-53 Rev. 5]

b. Restricting physical access and viewing of workstations (e.g., ensuring monitors are positioned away from public view or installing privacy screen filters or other physical barriers to prevent public viewing) to only authorized workforce members.
[45 C.F.R. § 164.310(c); CA SAM § 5365; NIST SP 800-53 Rev. 5]

c. Implementing policies and procedures for workstation, mobile device and media controls to prevent inadvertent loss or disclosure of health information when disposing of, or reusing workstations or mobile devices containing health information.
[45 C.F.R. § 164.310(d)(2); CA SAM § 5355, § 5365, and § 5365.3; NIST SP 800-53 Rev. 5]

3. Technical safeguards.

a. Enabling a password-protected screen saver or application that locks the screens of workstations, after a predetermined period of inactivity is acceptable for short duration session locking during business hours, so the workstation will be protected against unauthorized access. If the organization requires session termination (user logoff) for longer absences, such as overnight, an automated logoff capability should be implemented that can override the session lock (password-protected screen saver) after a predetermined period of inactivity.
[45 C.F.R. § 164.312(a)(2)(iii); NIST SP 800-53 Rev. 5]

b. Complying with all applicable password procedures. Best practices include passwords created with letters, numbers, and symbols.
[45 C.F.R. § 164.308(a)(5)(ii)(D)]

c. Implementing encryption policies and the use of approved encryption standards for health information.

Compensating control(s) or alternatives to encryption must be in place in the rare instances where encryption cannot be implemented.
[45 C.F.R. § 164.312(a)(2)(iv); CA SAM § 5350.1; NIST SP 800-53 Rev. 5]

d. Implementing secure configuration standards for hardware, software, and network devices to protect against reasonably anticipated threats or hazards to the security or integrity of health information, in compliance with state published standards, including the Email Threat Protection Standard.
[45 C.F.R. § 164.306(a)(2); CA SAM § 5315; CA SIMM § 5315-A]

e. Implementing procedures to authorize, and provide access to workstations in support of Technical Recovery Plan and Business Continuity Plan.
[45 C.F.R. § 164.312(a)(2)(ii)]

C. Documentation Retention. A state entity must retain any policy and procedure documentation related to workstation use and security, as well as any action, activity or assessment that is required to be documented by HIPAA for a minimum of six (6) years.
[45 C.F.R. §§ 164.316(b)(1) – (2)]

IV. References

45 C.F.R.

- § 164.306(a)
- § 164.308(a)
- § 164.310
- § 164.312
- § 164.316(b)

CA Health and Safety Code § 1280.18

CA SAM

- § 5305.4
- § 5305.5
- § 5315
- § 5315.6
- § 5315.7
- § 5335
- § 5335.2

- § 5350.1
- § 5355
- § 5355.1
- § 5360
- § 5360.2
- § 5365
- § 5365.3

CA SIMM § 5315-A

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Access Control
SHIPM Chapter 3 – Contingency Plans
SHIPM Chapter 3 – Device and Media Controls
SHIPM Chapter 3 – Encryption
SHIPM Chapter 3 – Facility Access Controls
SHIPM Chapter 3 – Information Access Management

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.3.0 – Technical Safeguards		
3.3.1 – Audit Controls		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide information regarding the security audit control measures to safeguard and protect health information against unauthorized access, use, disclosure or modification.

II. Policy

State entities must implement technical audit controls to monitor activity on their electronic systems that contain, or use, electronic health information.
[45 C.F.R. § 164.308(a)(1)(ii)(D), and § 164.312(b); CA SAM § 5305.2, and § 5335]

III. Implementation Specifics

State entities must consider their own risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use health information.

A. Policies and Procedures. State entities are responsible to develop and implement policies and procedures for regularly monitoring and reviewing audit records of their electronic information systems that contain, or use, electronic health information, to ensure that activity on those electronic systems is appropriate.
[45 C.F.R. § 164.308(a)(1)(ii)(D); CA SAM § 5305.2; CA SIMM § 5305-A]

B. Technical Mechanisms and Procedural Safeguards. State entities are required to implement hardware, software, and/or procedural mechanisms that record, and examine activity in information systems that contain, or use, electronic health information.
[45 C.F.R. § 164.308(a)(1)(ii)(D), and § 164.312(b)]

1. Technical Mechanisms. Technical mechanisms include, but are not limited to, audit trails (application, system-level, and user) and audit logs.

Examples of audit trails include:

a. Application audit trails normally monitor and log user activities in the application. This includes the application data files opened and closed, and the creating, reading, editing, and deleting of applications records associated with health information.

b. System-level audit trails usually capture successful or unsuccessful log-on attempts, log-on ID/username, date and time of each log-on/off attempt, devices used to log-on, and the application the user successfully or unsuccessfully accessed.

c. User audit trails normally monitor and log user activity in an electronic health information system or application by recording events initiated by the user, such as all commands directly initiated by the user, log-on attempts with identification and authentication, and access to electronic health information files and resources.

2. Procedural safeguards. Procedural safeguards include, but are not limited to:

a. Maintaining a regular and frequent review of audit trails and activity logs for electronic information systems containing electronic health information. Such activity may include log-on/off, file access, updates, edits and printing.

b. Investigate immediately any suspicious entries, such as unauthorized access or attempts to access electronic information systems containing health information.

c. Applying sanctions to workforce members for inappropriate activity related to accessing electronic information systems that contain health information.

d. Determining if workforce members are downloading executable files that may violate software-licensing agreements, or that may corrupt electronic information systems.

e. Verifying audit log integrity, to ensure it is accurate and has not been modified.

C. Documentation. A state entity must retain any policy and procedure documentation related to their technical audit controls, as well as any action, activity or assessment that is required by HIPAA, for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is greater.
[45 C.F.R. § 164.306, § 164.316(b)(1)(ii), and § 164.316(b)(2)(i)]

D. **ADDITIONAL STATE ENTITY REQUIREMENTS**

1. State entities are responsible to comply with their own internal information security policies to validate that appropriate security measures are in place, and functioning as intended. The validation shall include:

a. Ongoing assessments of key security measures and controls in both in-house and outsourced systems.
b. Completion of independent "pre-production" assessments of security controls in new systems or systems that are undergoing substantial redesign.
c. Adherence to the CA Office of Information Security (OIS) reporting requirements.
d. Coordination of all IT audit and assessment work done by third-party auditors.
e. Monitoring of third-party auditors' compliance to statewide information security requirements.

[CA SAM § 5330]

2. State entities are responsible to continuously identify and remediate vulnerabilities before they can be exploited. Vulnerability and threat management include, but are not limited to:
   a. Strategic placement of scanning tools to continuously assess all information technology assets.
   b. Implementation of appropriate scan schedules, based on asset criticality.
   c. Communication of vulnerability information to system owners or other individuals responsible for remediation.
   d. Dissemination of timely threat advisories to system owners or other individuals responsible for remediation.
   e. Consultation with system owners on mitigation strategies.
   f. Implementation of mitigation measures in accordance with the Vulnerability Management Standard.
   g. Implementation of minimum endpoint protection standards.

   [CA SAM § 5345, and 5355.1; CA SIMM § 5345-A, and 5355-A]

IV. References

45 C.F.R.

- § 164.306
- § 164.308(a)(1)(ii)(D)
- § 164.312(b)
- § 164.316(b)(1)(ii)
- § 164.316(b)(2)(i)

CA SAM

- § 5305.2
- § 5330
- § 5335
- § 5345
- § 5355.1

CA SIMM

- § 5305-A
- § 5345-A
- § 5355-A

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security Awareness and Training
SHIPM Chapter 4 – Administration
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter: 3 - Security		
Section: 3.3.0 – Technical Safeguards		
3.3.2 – Encryption		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding the requirements for encryption of computer systems and the protection against unauthorized access.

II. Policy

When health information is maintained electronically, policies and procedures must be implemented, and complied with, to ensure all of the following:

- Electronic information systems permit access only to persons or software programs that have been granted access rights.
- Protection against unauthorized access of health information when transmitted over an electronic communications network.
- Implement a mechanism to encrypt and decrypt electronic protected health information, when reasonable and appropriate to do so.

[45 C.F.R. § 164.312(a)(1), § 164.312(a)(2)(iv), and § 164.312(e)(1); CA SAM § 5350.1; NIST SP 800-53 Rev. 5]

III. Implementation Specifics

A. Policies and Procedures. State entities are responsible for implementing policies and procedures regarding the encryption methods their organization utilizes to prevent unauthorized access to health information.

B. Technical Safeguards. State entities are required to implement mechanisms to encrypt health information, in-transit or at rest, consistent with federal minimum encryption standards guidance.

1. In the rare instance, when it is not reasonable or appropriate to implement encryption, implement one or more alternative security measures (e.g., compensating controls) to accomplish the same purpose – consistent with CA SAM and the alternative to encryption approval process.
2. When neither encryption nor compensating controls are reasonable or appropriate to implement (following a thorough review of the organization's risk analysis, risk

mitigation strategy, other security measures already in place, and the cost of implementation), document the process and final decision.

Compensating controls and alternatives to encryption, must be reviewed on a case-by-case basis and approved in writing by the state entity's information security officer (ISO), after a thorough risk analysis.

[45 C.F.R. § 164.312(e)(2)(ii); CA SAM § 5350.1; NIST SP 800-53 Rev. 5]

C. Documentation and Retention. State entities are responsible to document and retain all of the following for a period of six (6) years from the date of its creation, or the data it was last in effect (whichever is greater):

1. Encryption policies and procedures documentation.
2. Any documentation related to compensating controls and alternatives to encryption (if applicable), including the state entity ISO written approval of such mechanisms.

[45 C.F.R. § 164.316(b)(2)(i)]

IV. References

45 C.F.R.

- § 164.312(a)(1)
- § 164.312(a)(2)(iv)
- § 164.312(e)(1)
- § 164.312(e)(2)(ii)
- § 164.316(b)(2)(i)

CA SAM § 5350.1

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Technical Safeguards

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.3.0 – Technical Safeguards		
3.3.3 – Access Administration (RETIRED June 2017)		
Review Date: N/A	Revision Date: N/A	Attachments: No

This policy was retired during the June 2017 SHIPM Update. This policy overlapped with content and requirements in 3.1.3 Information Access Management.

HIPAA requirements in this policy are now addressed in 3.1.3 Information Access Management.

Chapter: 3 – Security		
Section: 3.3.0 – Technical Safeguards		
3.3.4 – Integrity		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding the protection of health information against unauthorized access, modification or destruction.

II. Policy

Policies and procedures must be implemented to protect health information from unauthorized or improper access, alteration or destruction.
[45 C.F.R. § 164.312(c)(1), and § 164.312(e)(2)(i); CA SAM § 5310.5, and § 5315.5]

III. Implementation Specifics

A. State entities are responsible to implement policies and procedures that safeguard, and maintain the integrity of, health information from being improperly altered or destroyed during processing, in storage, or while in transit.
[45 C.F.R. §§ 164.312(c)(1) - (2), and § 164.312(e)(2)(i); CA Government Code § 11549.3; CA SAM § 5310.5, and § 5365.2; NIST SP 800-53 Rev. 5 and SP 800-66 Rev. 1]

B. Safeguards.

1. Implement mechanisms that authenticate access to health information, and corroborate that the information has not been altered or destroyed in an unauthorized manner.
[45 C.F.R. § 164.312(c)(2); CA SAM § 5315.5; NIST SP 800-66 Rev. 1]
2. Identify all approved users with the ability to access, alter or destroy data (see *SHIPM Chapter 3, Information Access Management*).
[NIST SP 800-66 Rev. 1]
3. Identify and address scenarios that may result in modification or destruction of health information by unauthorized sources (see SHIPM Chapter 3, *Security Management Process*).
[NIST SP 800-66 Rev. 1]

4. Implement measures to protect against unauthorized access, modification or destruction, to health information transmitted over an electronic communications network.
   [45 C.F.R. § 164.312(e)(2)(i); NIST SP 800-66 Rev. 1]

C. Documentation Retention. State entities are responsible to retain any policy and procedure documentation related to the integrity of health information, as well as any action, activity or assessment that is required to be documented by HIPAA for a minimum of six (6) years.
[45 C.F.R. §§ 164.316(b)(1) – (2)]

IV. References

45 C.F.R.

- §§ 164.312(c)(1) – (2)
- § 164.312(e)(2)(i)
- §§ 164.316(b)(1) – (2)

CA Government Code §11549.3

CA SAM

- § 5310.5
- § 5315.5
- § 5365.2

NIST

- SP 800-53 Rev. 5
- SP 800-66 Rev. 1

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Information Access Management
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 3 – Device and Media Controls
SHIPM Chapter 3 – Audit Controls

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.3.0 – Technical Safeguards		
3.3.5 – Access Control		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding the access control and administration measures that must be implemented to safeguard and protect health information against unauthorized access.

II. Policy

Technical policies and procedures must be developed, implemented, and maintained for electronic information systems that use electronic health information, to allow access only to those persons or software programs that have been granted access rights.
[45 C.F.R. § 164.308(a)(1)(ii)(B), § 164.308(a)(4), and § 164.312(a); CA SAM § 5305.5, § 5315.6, § 5315.8, § 5320.4, and § 5360.1]

III. Implementation Specifics

State entities are responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal access, activity, fraud, waste, and abuse in the use of information assets.

A. For all information systems that contain health information, policies and procedures must be implemented that limit access only to those persons or software programs that have been granted access rights according to applicable state and federal requirements. Access should be appropriate for the role and/or function of the person or software program. Policies and procedures must address all of the following:

1. Access rights, which at a minimum must be limited through use of the following:

   a. A unique name and/or number for identifying and tracking user identity and access. Assign a unique name and/or number for identifying and tracking user identity, based on the user identification and the authorization role (role-based access). Additionally, ensure the user has signed the appropriate user agreements before being granted access.
   [45 C.F.R. § 164.312(a)(2)(i); CA SAM § 5305.5, § 5315.8, § 5320.4, § 5360, and § 5360.1; NIST SP 800-53 Rev. 5]

b. Mechanisms to obtain necessary health information during an emergency. Procedures must be established to instruct workforce members on possible ways to gain access to needed health information to allow continuation of critical business processes and for the protection/security of health information while operating in emergency mode per the Business Continuity Plan.
[45 C.F.R. § 164.312(a)(2)(ii); CA SAM § 5325, and § 5325.2]

c. Termination of a session after a specified time of inactivity (automatic logoff). As a normal practice, workforce members and other users should logoff the system they are working on when their workstation is unattended. Enabling a password-protected screen saver or application that locks the screens of workstations after a predetermined period of inactivity is acceptable for short duration session locking during business hours. If the organization requires session termination (user logoff) for longer absences, such as overnight, an automatic logoff capability should be implemented that can after business hours session lock (password-protected screen saver) after a predetermined period of activity.
[45 C.F.R. § 164.312(a)(2)(iii); NIST SP 800-53 Rev. 5]

2. Encryption and decryption. State entities are responsible for implementing policies and procedures regarding the encryption methods their organization uses to prevent unauthorized access to health information (*see SHIPM Chapter 3, Encryption)*.
[45 C.F.R. § 164.312(a)(2)(iv); CA SAM § 5350.1]

B. Implement mechanisms to verify that a person or software programs seeking access to health information is the one claimed.

Note: Examples of technical mechanisms include:

1. Technical security measures to identify unauthorized access to health information
2. Clearly define and implement access restrictions and monitoring capabilities for cloud services
3. Documentation of health information to encrypt and decrypt, and the technical methods to prevent unauthorized access

C. Implement procedural safeguards to control access, and to prevent unauthorized access of health information.

Note: Examples of reasonable procedural safeguards include:

1. Track user activity within information systems based on user identification
2. Regular review of audit controls and access patterns
3. Enforce separation of duties and least privilege
4. Implement strict password and account management policies and procedures

5. Regular review of access rights for individuals and software programs
6. Monitor remote access from all end points, including mobile devices
7. Identify and maintain an inventory of information system connections

IV. References

45 C.F.R.

- § 164.308(a)
- § 164.312(a)

CA SAM

- § 5305.5
- § 5315.6
- § 5315.8
- § 5320.4
- § 5325
- § 5325.2
- § 5350.1
- § 5360
- § 5360.1

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Contingency Plans
SHIPM Chapter 3 – Information Access Management
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 3 – Encryption

VI. Attachments

None

Chapter: 3 – Security		
Section: 3.4.0 – Policy and Procedures		
3.4.1 - Documentation		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: Yes

I. Purpose

To describe the requirements for the development and implementation of security policies and procedures, to safeguard and protect health information, regardless of its form (electronic, optical, oral, print or other media).

II. Policy

Security policies and procedures must be developed, implemented, utilized and maintained to ensure the confidentiality, integrity, and availability of health information that is created, received, maintained, or transmitted.

[45 C.F.R. §§ 164.316(a) – (b); CA Civil Code § 56.101, and § 1798.21; CA Health and Safety Code § 1280.15, and § 123149; CA SAM § 5300.5, § 5305, and § 5315.3]

III. Implementation Specifics

A. State entities should consider all of the following when developing and implementing information security policies and procedures:

1. The size, complexity, and capabilities of the organization
2. The technical infrastructure, hardware, and software security capabilities of the organization
3. The costs of implementing security measures
4. The probability and criticality of potential risks to health information that the organization creates, receives, maintains or transmits electronically

[45 C.F.R. §§ 164.306(b)(2)(i) – (iv)]

B. Security policies and procedures shall address the following standards (shown in the following tables):

Administrative Safeguards	Specifics	45 C.F.R. § 164.308	CA SAM § 5300
Security Management Process	Risk Analysis	R	R
	Risk Management	R	R
	Sanction Policy	R	R
	Information System Activity Review	R	R
Assigned Security Responsibility	Assigned Security Responsibility	R	R
Workforce Security	Authorization and/or Supervision	A	R
	Workforce Clearance Procedure	A	R
	Termination Procedures	A	R
Information Access Management	Isolating Healthcare Clearinghouse Function	R	R
	Access Authorization	A	R
	Access Establishment and Modification	A	R
Security Awareness and Training	Security Reminders	A	R
	Protection from Malicious Software	A	R
	Log-in Monitoring	A	R
	Password Management	A	R
Security Incident Procedures	Response and Reporting	R	R
Contingency Plan	Data Backup Plan	R	R
	Disaster Recovery Plan	R	R
	Emergency Mode Operation Plan	R	R
	Testing and Revision Procedures	A	R
	Applications and Data Criticality Analysis	A	R
Evaluation	Evaluation	R	R
Business Associate Contracts	Written contract or other arrangement	R	R

Physical Safeguards	Specifics	45 C.F.R. § 164.310	CA SAM § 5300
Facility Access Controls	Contingency Operations	A	R
	Facility Security Plan	A	R
	Access Control and Validation Procedures	A	R
	Maintenance Records	A	R
Workstation Use	Workstation Use	R	R
Workstation Security	Workstation Security	R	R
Device and Media Controls	Disposal	R	R
	Media Re-use	R	R
	Accountability	A	R
	Data Backup and Storage (during transfer)	A	R
Technical Safeguards	**Specifics**	**45 C.F.R. § 164.312**	**CA SAM § 5300**
Access Control	Unique User Identification	R	R
	Emergency Access Procedure	R	R
	Automatic Logoff	A	R
	Encryption and Decryption (including data at rest)	A	R
Audit Controls	Audit Controls	R	R
Integrity and Implementation Process	Mechanism to authenticate ePHI	A	R
Person or Entity Authentication	Person or Entity Authentication	R	R
Transmission Security	Integrity Controls	A	R
	Encryption (FTP and email over internet)	A	R

R = **required** - the specification must be implemented

A = **addressable** – state entities must use reasonable and appropriate measures to meet the implementation specification. Organizations must complete one of the following with appropriate documentation:

1. Implement the addressable implementation specifications if reasonable and appropriate.

2. If implementing the specification is not reasonable and appropriate, the organization must either:
   a. Implement one or more alternative security measures to accomplish the same purpose, or
   b. Not implement either an addressable implementation or an alternative, if the standard could still be met, and justify in writing why the implementation specification would not be reasonable or appropriate.

C. State entities must make the necessary documentation available to those workforce members responsible for implementing the entity's security policies and procedures.
[45 C.F.R. § 164.316(b)(2)(ii)]

D. State entities must maintain any policies and procedures by completing the following:
   1. Periodically review and update as needed in response to environmental or operational changes affecting the security of health information.
   2. Document (security policies and procedures) in written form, which may be electronic, and keep or maintain a minimum of six (6) years.

      Outdated policies and procedures must be kept as documentation of compliance for at least six (6) years from the date of creation, or the date when the policy and procedure was last in effect, whichever is later.

[45 C.F.R. § 164.316(b)(1), § 164.316(b)(2)(i), and § 164.316(b)(2)(iii)]

E. State entities shall apply all applicable statewide and state entity information security laws, policies, standards, and procedures in order to protect health information under the information asset owner's responsibilities.
[CA SAM 5310.7]

F. State entities that have electronic health record systems (EHRs) or electronic medical record systems (EMRs) must do both of the following:
   1. Protect and preserve the integrity of electronic health information.
   2. Automatically record and preserve any change or deletion of any electronically stored health information.

[CA Civil Code § 56.101]

IV. References

45 C.F.R.

- §§ 164.306(b)(2)(i) – (iv)
- §§ 164.308 – 164.312
- § 164.316

CA Civil Code

- § 56.101
- § 1798.21

CA Health and Safety Code

- § 1280.15
- § 123149

CA SAM §§ 5300 - 5365.3

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Policies and Procedures
SHIPM Chapter 4 – Business Associates

VI. Attachments

Yes - SHIPM Required Policies and Procedures Checklist

Chapter 4 – Administrative

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.1 – Policies and Procedures		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: Yes

I. Purpose

To ensure compliance with state and federal requirements to maintain current, written policies and procedures regarding privacy and confidentiality of health information.

II. Policy

Health information must be safeguarded from inappropriate access, use, or disclosure by maintaining current privacy policies and procedures, and ensuring workforce members comply with them. These privacy policies and procedures must:

- Demonstrate compliance with California's SHIPM
- Be consistent with the entity's Notice of Privacy Practices (NPP)
- Be compliant with state and federal requirements for use and disclosure of health information, including laws and regulations specific to individual departments
- Address any applicable reporting requirements, such as those for abuse, neglect, or communicable disease reporting

[45 C.F.R. § 164.306, § 164.316, and § 164.530; CA Civil Code §§ 1798–1798.99; CA Health and Safety Code § 1280.18; CA SAM §§ 5300 – 5365.3]

III. Implementation Specifics

A. State entities are responsible to develop and maintain operational privacy policies and procedures that are compliant with the SHIPM.

1. Required scope of privacy policies and procedures. Current privacy policies and procedures (which may be in electronic form or in hard paper copy) must be maintained and designed to comply with federal and applicable state privacy requirements. The privacy policies and procedures must cover and specify all of the following:

   a. All persons in the state entity who are involved in the design, development, operation, disclosure, or maintenance of records containing health information

   b. All legally permissible and prohibited uses and disclosures of, and requests for health information the state entity is likely to make and how the state entity handles each

2. Operational privacy policies and procedures must clearly address all of the following:
   a. The person or persons in the organization responsible for development and implementation of the privacy policies and procedures
   b. When health information would, or would not, be disclosed to entities external to the organization
   c. Who is responsible for carrying out each specific privacy-related activity and where in the organization the activity is to be performed
   d. How the documentation requirements are met (*see III.A.7 below*)
   e. The timeframes for performing each privacy-related activity
   f. How compliance with the NPP is achieved
   g. How any business associates or contractors are informed of the required privacy policies and procedures
   h. Breach policy and procedures
   i. Rules of conduct for persons involved in the design, development, operation, disclosure or maintenance of records containing health information
3. Training. Workforce members must receive training within a reasonable period of time after any material change to the privacy policies and procedures becomes effective.
4. Changes. Changes must be made promptly to the privacy policies and procedures if necessary to comply with changes in law or business practices.

   While not required, it is recommended and a best practice to expressly state in the NPP that the state entity reserves the right to make changes in actual practice in advance of updating the NPP.

   Unless this right is stated in the NPP, the state entity must update the NPP prior to making the actual procedural change. Other changes that are not material may be made at any time if applicable documentation requirements are met, including changes to the privacy policies and procedures.
5. Complaints. State entities are responsible to provide a process for a patient to make complaints concerning the privacy policies and procedures, the state entity's compliance with its own policies, and/or any privacy provisions the state entity has or has not implemented.
6. Sanctions. Workforce members who fail to comply with the privacy policy and procedures of the state entity, shall be subject to disciplinary action(s), as appropriate.

7. Documentation and maintenance. Privacy policies and procedures must be maintained in writing, which includes electronic storage. Paper records are not required. State entities are responsible to do all of the following:
   a. Document training provided
   b. Document any sanctions or discipline due to non-compliance with privacy policies and procedures
   c. Retain documentation of privacy policies and procedures for at least six (6) years from the date of their creation or the date when it was last in effect, whichever is later
   d. Make privacy policies and procedures available to staff responsible for implementing them
   e. Review privacy policies and procedures at least annually and update them as needed
8. State entities shall apply all applicable statewide and state entity information security laws, policies, standards, and procedures in order to protect health information under the information asset owner's responsibilities.
   [CA SAM 5310.7]

IV. References

45 C.F.R.

- § 164.306
- § 164.316
- § 164.530

CA Civil Code §§ 1798–1798.99

CA Health and Safety Code § 1280.18

CA SAM §§ 5300-5365.3

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 4 – Privacy Training
SHIPM Chapter 4 – Staffing: Privacy Official, Security Official
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

Yes - SHIPM Required Policies and Procedures Checklist

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.2 – Privacy Training		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance for all workforce members regarding the required privacy training, about the organizations policies and procedures that protect health information, consistent with each workforce member's job responsibilities and functions.

II. Policy

Formal education and training on privacy policies and procedures must be provided to all workforce members to prepare them to understand and carry out their job functions.
[45 C.F.R. §§ 164.530(b)(1) – (2); CA SAM § 5320]

III. Implementation Specifics

A. State entities are responsible to provide training to all workforce members regarding their implemented privacy policies and procedures.

The scope and content of the training, or periodic (and at least annually) refresher training, should target the workforce member's specific job functions.

The privacy training must:

1. Be provided to each new workforce member within 30 days of beginning service and prior to accessing health information.
   [45 C.F.R. § 164.530(b)(2)(i)(B); CA SAM § 5320.1]
2. Be provided within a reasonable period of time after a material change in the policies and procedures becomes effective.
   [45 C.F.R. § 164.530(b)(2)(i)(C)]
3. Be documented in writing, which may be an electronic training record, and include which workforce members were trained, topics covered, and training dates.
   [45 C.F.R. § 164.530(b)(2)(ii), and §§ 164.530(j)(1) - (2)]
4. Establish rules of conduct and instruct each workforce member about the rules and procedures concerning the privacy of individuals' information.
   [CA Civil Code § 1798.20]

B. State entities that are hybrid entities need to provide training to workforce members in those portions of the organization designated as covered components (functions).

C. Documentation requirements. State entities are responsible to document all of the following:

1. Privacy training materials. Be provided within a reasonable period of time after a material change in the policies and procedures (i.e., changes in business practices, legislative or regulatory changes) becomes effective. In addition, review training materials at least annually and update as needed.
[45 C.F.R. § 164.530(b)(2)(i)(C); CA SAM § 5320.3]

2. Privacy training records. Document the workforce member who received training, topics covered and training dates to ensure tracking and corrective actions.
[45 C.F.R. § 164.530(b)(2)(ii); CA SAM § 5320.3]

3. Retention. State entities are responsible to retain privacy training documentation for six (6) years from the date of its creation, or the date when it last was in effect, whichever is later.
[45 C.F.R. §§ 164.530(j)(1) – (j)(2)]

IV. References

45 C.F.R.

- §§ 164.530(b)(1) – (2)
- §§ 164.530(j)(1) – (2)

CA Civil Code § 1798.20

CA SAM § 5320

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security Awareness and Training
SHIPM Chapter 4 – Policies and Procedures

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.3 – Sanctions for Violation		
Review Date: 06/01/2017	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To provide guidance regarding required sanctions which must be included in policy, and applied against any workforce member who views, uses, or discloses health information outside of the constraints of their position or does not follow policy.

II. Policy

Policies and procedures must specify appropriate sanctions outlining what the consequences will be against any workforce member who improperly views, uses, or discloses health information.

State entities are encouraged to consult with their labor relations or Human Resources departments prior to developing and applying operational policies and procedures governing workforce sanctions for violating privacy and security policies.
[45 C.F.R. § 164.308(a)(1)(ii)(C); CA Health and Safety Code § 1280.18; CA Civil Code § 1798.21]

III. Implementation Specifics

A. State entities are responsible to implement, maintain, and apply written policies which contain all the following required elements:
   1. Language that outlines specific sanctions against and consequence to, any workforce member who fails to comply with security and privacy policies by improperly viewing, using, disclosing, or allowing access to health information.
   2. The sanction language should be included in any training materials provided to workforce members.
   3. Language that specifically states the sanctions must be appropriate to the severity of the violation, up to and including termination.
   4. Language that, depending on the severity of the violation, law enforcement notification may be required.

5. Language about civil sanctions and penalties. The policy must state that workforce members can be charged with a misdemeanor, or suffer fines and civil penalties, depending on the economic loss to the patient and the degree of malice.

[45 C.F.R. § 164.308(a)(1)(ii)(C), and § 164.530(e)(1); CA Civil Code § 56.36, and §§ 1798.55 –1798.57]

B. Whistleblower and victims of crime exemptions. Federal law allows a workforce member to disclose health information without an authorization in certain situations (e.g., state entity or business associate is engaging in illegal conduct, etc.). *See SHIPM Chapter 2, Victims of Abuse, Neglect, or Domestic Violence.*

Please refer to your organization's legal counsel for guidance on Victims of Crime exception matters.

[45 C.F.R. § 164.502(j); CA Civil Code § 56.10(c)(14), § 1798.24(e), § 1798.24(j), and § 1798.24(o)]

C. Documentation. State entities are responsible to document any sanctions that were applied, and maintain the documentation for a minimum of six (6) years. *[45 C.F.R. § 164.530(e)(2)]*

IV. References

45 C.F.R.

- § 164.308
- § 164.502(j)
- § 164.530(e)(i)
- § 164.530(e)(2)

CA Civil Code

- § 56.10(c)(14)
- § 56.36
- § 1798

CA Health and Safety Code § 1280.18

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 2 – Minimum Necessary

SHIPM Chapter 3 – Incident Procedures
SHIPM Chapter 3 – Security Awareness and Training
SHIPM Chapter 3 – Workstation Use and Security
SHIPM Chapter 3 – Encryption
SHIPM Chapter 3 – Access Control

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.4 – Staffing: Privacy Official, Security Official		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe certain workforce staffing roles required within an organization to support health information privacy and security compliance.

II. Policy

Specific workforce roles related to privacy and security must be designated and documented in job duty statements to ensure privacy and security policies and procedures are developed, implemented, followed, and maintained.

III. Implementation Specifics

A. State entities are responsible to designate all the following workforce staffing roles:

1. Privacy Official. A privacy official must be designated to be responsible for the development, implementation, and compliance with the state entity's policies and procedures relating to privacy. Responsibilities include, but are not limited to: [1]
   a. Assists in the development and implementation of privacy policies and procedures
   b. Ensures compliance with privacy policies and procedures, and legal requirements
   c. Performs ongoing compliance monitoring activities
   d. Works with legal counsel and management to ensure forms, authorizations, and notices are current
   e. Ensures adequate privacy training
   f. Assists with, coordinates, or tracks staff member access to health information
   g. Ensures patient's right to access, amend and restrict access to their protected health information (PHI)

[1] Responsibilities paraphrased and quoted from information found on the American Health Information Management Association (AHIMA) website

h. Ensures a process for addressing complaints on privacy policies and procedures, including complaints on denial of access to PHI
i. Coordinates with the Security Official
j. Maintains current knowledge of applicable federal and state privacy laws and standards
k. Answers and addresses privacy questions and issues
l. Leads efforts for breach determination and notification processes under HIPAA and applicable State breach rules and requirements
m. Coordinates and cooperates with the U.S. Department of Health and Human Service (HHS) Office for Civil Rights (OCR), CalOHII, State regulators and/or other legal entities, and organization or officers in any compliance reviews or investigations
n. Partners with Security Official to recommend sanctions for privacy violations
o. Performs or oversees initial and periodic information privacy risk assessment/analysis, mitigation and remediation
p. Participates in the development, implementation, and ongoing compliance monitoring of business associates (BAs) and business associate agreements (BAAs), to ensure privacy concerns, requirements, and responsibilities are addressed

[45 C.F.R. § 164.530(a)(1)(i)]

2. Privacy Notice Contact Person or Office**.**
   a. A contact person or office must be identified with their name (or title) and telephone number in any notice describing how a patient's health information may be used and disclosed, and how the patient can get access to their information *(see SHIPM Chapter 5, Notice of Privacy Practices*)
   b. The designated contact person or office is responsible for receiving privacy-related complaints and providing additional information about the content of the privacy notice

   [45 C.F.R. § 164.520(b)(1)(vii), and § 164.530(a)(1)(ii)]
3. Security Official. A security official must be identified who is responsible for development and implementation of an entity's policies and procedures relating to security. Responsibilities include, but are not limited to:[2]

[2] Responsibilities paraphrased and quoted from information found on the American Health Information Management Association (AHIMA) website

a. Builds a strategic and comprehensive information security program that defines, develops, maintains and implements policies and processes that enable consistent, effective information security practices which minimize risk and ensure the integrity, confidentiality and availability of information that is owned, controlled or processed within the organization. Ensures information security policies, standards, and procedures are up-to-date
b. Initiates, facilitates, and promotes activities to foster information security awareness within the organization
c. Creates a culture of cyber security both with the IT organization and driving behavioral changes for the business
d. Evaluates security trends, evolving threats, risks and vulnerabilities and applies tools to mitigate risk as necessary
e. Manages security incidents and events involving electronic protected health information (ePHI)
f. Ensures that the technology recovery, business continuity, risk management and access controls needs of the facility are addressed
g. Ensures the institution/organization complies with the administrative, technical and physical safeguards
h. Works closely with the Privacy Official to ensure alignment between security and privacy compliance programs including policies, practices and investigations, and acts as a liaison to the information systems and compliance departments
i. Responsible for initial and periodic information security risk assessment/analysis, mitigation and remediation. Responsible for development and implementation of security risk management plan
j. Ensures organization has audit controls to monitor activity on electronic systems that contain or use electronic protected health information
k. Oversees periodic monitoring and reviewing of audit records to ensure that system activity is appropriate. Such activity would include, but is not limited to, logons and logoffs, file accesses, updates, edits and printing
l. Ensures the organization has and maintains appropriate system use and disclosure/confidentiality statement
m. Oversees, develops and/or delivers initial and ongoing security training to the workforce. Initiates, facilitates and promotes activities to foster information security awareness within the organization and related entities
n. Participates in the development, implementation, and ongoing compliance monitoring of business associates (BAs) and business associate agreements

(BAAs), to ensure security concerns, requirements, and responsibilities are addressed

o. Assists Privacy Official as needed with breach determination and notification processes under HIPAA and applicable State breach rules and requirements

p. Establishes and administers a process for investigating and acting on security incidents which may result in a privacy breach

q. Partners with Privacy Official to recommend sanctions for security violations

r. Maintains current knowledge of applicable federal and state security laws, licensing and certification requirements and accreditation standards

s. Cooperates with the HHS OCR, CalOHII, State regulators and/or other legal entities, and organization or officers in any compliance reviews or investigations

t. Performs or oversees initial and periodic information security risk assessment/analysis, mitigation, and remediation

[45 C.F.R. § 164.308(a)(2); CA SAM § 5305.3]

B. Each state entity has different business needs depending on size and workload. Although there are no statutory restrictions against the same person filling more than one of the above roles, CalOHII recommends the above roles are filled by separate people. Ultimately, state entities are responsible to assess what allocation of time and resources will adequately support the workload commensurate with each role.

C. **ADDITIONAL STATE ENTITY REQUIREMENTS**

Establish an entity-wide information security, privacy and risk management strategy/program.

[CA SAM § 5305.5, and § 5310]

IV. References

45 C.F.R.

- § 164.308(a)(2)
- § 164.520(b)(1)(vii)
- § 164.530(a)(1)(i) – (ii)

CA SAM

- § 5305.3
- § 5305.5
- § 5310

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Privacy Training
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.5 – Trading Partner Agreements		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the responsibilities for the use of trading partner agreements (TPAs), related to the electronic data interchange (EDI) of health information.

II. Policy

TPAs are used to specify technical requirements not included in a business associate agreement (BAA). These technical details must be followed during the electronic exchange of health information between entities (e.g., ANSI x12 electronic health transactions standards).

[45 C.F.R. § 160.103, § 162.103, and § 162.915]

III. Implementation Specifics

A. State entities that are business associates (BAs), health care clearinghouses, health care plans, health care providers, or hybrid entities that use TPAs are responsible to ensure that such agreements do not do any of the following:

1. Change the definition, data condition, or use of a data element or segment in a standard, except where necessary to implement state or federal law, or to protect against fraud and abuse.
2. Add any data elements or segments to the maximum defined data set.
3. Use any code or data elements that are either marked "not used" in the HIPAA standard's implementation specification or are not in the HIPAA standard's implementation specification(s).
4. Change the meaning or intent of the standard's implementation specification(s).

B. It is recommended that the TPA include or reference a Companion Guide to define specific details, requirements, processes and implementation steps in accordance with the HIPAA Implementation Guides for the applicable electronic transactions. In addition, the Companion Guide also includes general information and instructions on electronic data interchange, including, but not limited to, communications protocols, testing, requirements, and acknowledgments.

IV. References

45 C.F.R.

- § 160.103
- § 162.103
- § 162.915

HIPAA Implementation Guides American National Standards Institute (ANSI) Standards

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 4 – Transactions and Code Sets (TCS)
SHIPM Chapter 4 – Business Associates
SHIPM Chapter 4 – Providers, Employers Identifiers

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.1.0 – Administrative Requirements		
4.1.6 – Waiver of Rights Related to HIPAA Complaints		
Review Date: 06/01/2016	Revision Date: 06/01/2016	Attachments: No

I. Purpose

To explain that a patient cannot waive his or her right to file complaints for non-compliance with privacy, security, or patients' rights requirements.

II. Policy

A patient always has the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services (HHS) if she or he believes there has been noncompliance with requirements. It is prohibited to request that a patient waive this right for any reason; this right *cannot be waived.*

III. Implementation Specifics

A. State entities that are business associates (BAs), health care clearinghouses, health care plans, health care providers, or hybrid entities shall not require any patient to waive his or her right to file a complaint with the Secretary of HHS, as a condition of the provision of treatment, payment, enrollment in a health care plan, or eligibility for benefits.
[45 C.F.R. § 164.306, § 164.530(d), § 164.530(g), and § 164.530(h)]

IV. References

45 C.F.R.

- § 164.306
- § 164.530(d)
- § 164.530(g)
- § 164.530(h)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Treatment, Payment and Health Care Operations (TPO)

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.2.0 – Compliance		
4.2.1 – Consequences of Non-Compliance		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To describe the responsibilities related to compliance activities, and the possibility of consequences (e.g., criminal convictions, administrative fines and civil monetary penalties) which may be applied, should a court or a federal or state oversight agency determine the use or disclosure of health information is not compliant with laws and regulations.

II. Policy

State entities, as well as their business associates (BAs), workforce members and agents, are required to cooperate with federal and state agencies responsible for determining compliance with HIPAA and other laws relating to the privacy, security, and administration of health information.
[45 C.F.R. § 160.402, § 160.404, and § 160.410]

III. Implementation Specifics

The U.S. Department of Health and Human Services (HHS) is authorized by law to determine compliance with HIPAA, and other federal laws relating to privacy, security, transactions and code sets (TCS), and the administration of health information.
[45 C.F.R. § 160.300, and §§ 160.302 – 160.308]

A. State entities are responsible to support and cooperate with HHS compliance activities. Specifically, state entities are responsible to do all of the following:
   1. Provide records and compliance reports. A state entity must keep records and submit compliance reports in a time and manner requested by HHS, to ascertain whether the state entity complies with federal regulations regarding health information
   2. Cooperate with complaint investigations and compliance reviews. A state entity must cooperate with an HHS investigation or compliance review of the entities policies, procedures, or practices, to determine whether it is complying with federal regulations regarding health information
   3. Permit access to information. A state entity must permit access by HHS during normal business hours to its facilities, books, records, accounts, and other sources

of data that are pertinent to ascertaining compliance with regulations regarding health information

Health information obtained by HHS or its agents in connection with this type of investigation or compliance review, shall not be subsequently disclosed, unless necessary for ascertaining or enforcing compliance, or if otherwise required by law. *[45 C.F.R. § 160.310]*

B. Non-compliance due to acts by BAs (or agents). State entities are responsible for all violations by their BAs. BAs are also responsible for the acts of their agents. *[45 C.F.R. § 160.402(c)]*

State entities may be held responsible for their BAs' actions. As a result, state entities must be reasonably diligent to ensure that BAs are compliant (e.g., use of appropriate business associate agreements), and BAs are responsible to do the same for their subcontractors *(see SHIPM Chapter 4, Oversight of Business Associates*).

C. The State of California Office of Health Information Integrity (CalOHII) is authorized by law to coordinate implementation and compliance activities within state government for HIPAA and other laws relating to privacy, security, and administration of health information.
[CA Health and Safety Code § 130310]

State entities are also responsible to support and cooperate with CalOHII's coordination and compliance activities. Specifically, state entities, BAs, their workforce members, and agents are required to comply with all of the following:

1. Respond in a timely and complete manner to all activities undertaken to assess and ensure HIPAA implementation, progress and compliance with HIPAA, and other laws and policies relating to health information.

   Required responses from state entities include, but are not limited to:

   a. Assisting in periodic statewide assessments

   b. Providing documentation or information upon request in the format requested

   [CA Health and Safety Code § 130310, and § 130311]

2. Comply with the decisions of the CalOHII director in achieving compliance with HIPAA.
   [CA Health and Safety Code § 130311]

D. HHS violation penalty considerations. An HHS finding that an individual or organization failed to comply with HIPAA and/or other regulations regarding health information may result in criminal convictions, administrative fines and civil penalties.

In determining the type and size of the penalty, HHS may consider any of the following as aggravating or mitigating factors, as appropriate:

1. The nature and extent of the violation, including the number of patients affected and the time period during which the violation occurred
2. The nature and extent of the harm resulting from the violation (such as financial impact or damage to patient's reputation)
3. The history of prior compliance, including previous violations
4. The financial condition of the entity or BA, including whether financial difficulties affected the ability to comply, and whether the imposition of the penalties would risk ability to continue to provide or pay for health care

[45 C.F.R. § 160.408]

HHS annually updates the civil monetary penalties associated with non-compliance pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015. In addition to financial penalties, a sentence of up to 10 years of prison time is possible for individuals who are non-compliant with intent to sell, transfer, or use health information for commercial advantage, personal gain, or malicious harm.
[42 U.S.C. § 1320d–5; 45 C.F.R. § 102.3, § 160.404, and § 160.406]

E. Additional State of California penalties. In addition to federal law, California law identifies possible penalties for non-compliance, including criminal convictions and administrative fines (or civil monetary penalties) to individuals and organizations ranging from $1,000 up to $250,000 for illegally disclosing health information.
[CA Civil Code § 56.10(a), § 56.35 – 56.36, § 1798.24, and §§ 1798.55 - 1798.57]

F. Documentation and retention. State entities are responsible to document any official findings of non-compliance by a state or federal compliance oversight entity, and any penalties that are imposed for non-compliance. Documentation must be maintained for six (6) years.
[45 C.F.R. § 164.530(e), and § 164.530(j)]

IV. References

42 U.S.C. § 1320d–5

45 C.F.R.

- § 102.3
- § 160.300
- §§ 160.302 – 160.308
- § 160.310
- § 160.402
- § 160.404
- § 160.406
- § 160.408

- § 160.410
- § 164.530(e)
- § 164.530(j)

CA Civil Code

- § 56.10(a)
- §§ 56.35 – 56.36
- § 1798.24
- §§ 1798.55 – 1798.57

CA Health and Safety Code

- § 130310
- § 130311

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 1 – State Agency Responsibilities
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Oversight of Business Associates

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.3.0 – Transactions and Code Sets		
4.3.1 – Transactions and Code Sets (TCS)		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the use of HIPAA's standardized transactions and code sets (TCS) in the electronic data interchange (EDI) of health information.

II. Policy

When health information is moved electronically for certain administrative and financial reasons, TCS standards must be used.
[45 C.F.R. §162.923, § 162.925, and § 162.930]

III. Implementation Specifics

A. State entities are responsible to use current standard electronic transactions, identifiers, and code sets to exchange health information electronically including, but not limited to:

1. Standard electronic transactions:
   a. ASC X12 837 – Health care claims and coordination of benefits (or equivalent encounter information) for dental, professional and institutional
   b. ASC X12 270/271 – Eligibility for a health care plan (request and response) for dental, professional and institutional
   c. ACS X12 276/277 – Health care claim status (request and response)
   d. ACS X12 834 – Enrollment and disenrollment in a health care plan
   e. ASC X12 835 – Health care payment and remittance advice
   f. ASC X12 820 – Health care plan premium payment
   g. ACS X12 278 – Referral certification and service authorization (request and response)
   h. NCPDP D.0 COB – Coordination of benefits (COB)
   i. NCPDP D.0 – Health care claims, eligibility, or referral certification and authorization for retail pharmacy drug

j. NCPDP 5.1 and NCPDP D.0 – Retail pharmacy drug claims (telecommunication and batch standards)

k. NCPDP 3.0 – Medicaid pharmacy subrogation (batch standard)

[45 C.F.R. §§ 162.900 - 162.1902]

2. Unique Identifiers. There are national identification number requirements for use with the standard electronic transactions *(see SHIPM Chapter 4, Provider, Employers Identifiers*), listed above:

   a. Providers

   b. Employers

3. Medical code sets. The following medical code sets must be used with the standard electronic transactions, listed above:

   a. International Classification of Diseases (ICD-10-CM) is used for reporting diagnosis and inpatient hospital procedures. The ICD is the international standard for defining and reporting diseases and health conditions

   b. Health Care Financing Administration Common Procedure Coding System (HCPCS) and the Current Procedure Terminology (CPT-IV), are used by health care providers and health care plans in conjunction with medical billing processes to identify procedures and services

   c. National Drug Codes (NDC) for drugs and biologics is used to identify each medication listed in the U.S. Federal Food, Drug and Cosmetic Act

   d. The American Dental Association's Codes on Dental Procedures and Nomenclature for dental services

   [45 C.F.R. §§ 162.1000 - 162.1011]

B. Security and privacy. State entities are responsible to comply with all of the other SHIPM policies pertaining to Privacy, Security, Administrative Requirements and Patient Rights (see *SHIPM Chapters 2, 3, 4, and 5*).

C. Electronic Signature. State entities are responsible to comply with the information security and privacy policies, standards, and procedures issued by the Office of Information Security (OIS).
[CA SAM § 5300.2]

D. Electronic transfer of information between multiple health care plans. State entities are responsible to adopt standards for transferring appropriate standard data elements needed for the coordination of benefits, sequential processing of claims and other data elements between health care plans for those patients who have more than one (1) health care plan.

E. It is recommended that TCS standards and processes are documented in a Companion Guide.

IV. References

45 C.F.R. §§ 162.900 - 162.1902

CA SAM § 5300.2

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.4.0 – Business Associates		
4.4.1 – Business Associate Agreement		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: Yes

I. Purpose

To provide guidance regarding the contractual requirements that allow for the sharing or disclosure of health information with business associates (BAs).

II. Policy

BAs need access to health information to carry out, assist with the performance of, or perform a function or activity on behalf of a state entity. A state entity is responsible to have a contract or other written agreement with its BA. When a business associate agreement (BAA) is executed, a state entity may permit BAs to use or disclose health information (e.g., create, receive, access, maintain, and transmit) on the state entity's behalf.

A state entity that is a covered entity can also be the BA of another covered entity, if they perform duties on behalf of that covered entity.
[45 C.F.R. § 164.308(b), §§ 164.314(a)(1) - (2), § 164.502, § 164.504, § 164.504(e)(2), and § 164.504(e)(3)(i); CA SAM § 5305.8, and § 5310.3; NIST SP 800-53 Rev. 5]

III. Implementation Specifics

A. A BA is permitted to use or disclose health information only in the manner specified in an executed legal agreement between their organization and the state entity. This includes information about any restrictions for the use or disclosure of information as requested by the patient as well as any requests by the patient regarding Confidential Communications (*see SHIPM Chapter 5, Confidential Communications*).

B. Each state entity may have specific program requirements that may need to be incorporated into the BAA, Memorandum of Understanding (MOU), or Interagency Agreement (IA).

C. The BAA must provide that the BA will comply with all applicable requirements. *[45 C.F.R. § 164.314]*

D. When a covered entity engages the services of a cloud services provider to create, receive, maintain, or transmit electronic protected health information (ePHI) (such as to process and/or store ePHI), on its behalf, the cloud services provider is a BA under

HIPAA. As a result, the covered entity (or BA) and the cloud services provider must enter into a HIPAA-compliant BAA, and the cloud services provider is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA rules.
[CA SAM § 4983, and §4983.1]

E. State entities that share health information with other government entities, may utilize an MOU or IA as the legal instrument that specifies the contractual requirements with regard to handling and safeguarding health information. These MOUs or IAs must contain certain minimum provisions required in a BAA between covered entities and their BAs.

F. Whenever there is a change in the law affecting what is required in a BAA, the document must be updated.

G. BAA templates must be reviewed and updated often enough to ensure they are accurate and consistent with the law, and distributed to all units within your organization that use the templates to ensure updated templates are being used.

H. State entities may have requirements for the BA to provide specific documentation in support of ongoing audits, inspection, enforcement, oversight and risk management activities to monitor and ensure compliance. For example, the documentation requested for the BA may include Technology Recovery Plan, Business Continuity Plan, completed risk analysis, Plan of Action and Milestones (POAM), etc.

I. BAAs must contain language that requires the BA to do all of the following:
   1. Maintain the confidentiality, integrity, and availability of all health information that the BA uses or discloses.
   2. Follow the permitted and required uses and disclosures of health information as specified in the BAA. The agreement:
      a. Must state the purpose for which use or disclosure is:
         i. Permitted
         ii. The rationale for these permissions
         iii. To whom the BA may make further disclosures
      b. Is *not* required to list each specific item for which use or disclosure is permitted
      c. Cannot authorize the BA to use or further disclose health information in a manner that violates state or federal law
      d. May permit the BA to use or disclose the health information for either of the following:
         i. To carry out the legal responsibilities of the BA, or

ii. For the proper management and administration of the BA, consistent with federal and state laws.

e. May permit the BA to provide data aggregation services related to the health care operations of the state entity only

3. Ensure a BA's use of software to identify patterns in large batches of data (also known as "data mining"), for any purpose not specified in the BAA, MOU, or IA, is documented as a violation of the agreement and grounds for termination of the agreement by the state entity.
4. Protect against any reasonably anticipated threats or hazards to the security or integrity of health information by using physical, technical, and administrative safeguards.
5. Protect against any reasonably anticipated uses or disclosures of health information that are either of the following:
   a. Not permitted or required by state or federal requirements, or
   b. Not provided for by the BAA, MOU, or IA.
6. Ensure ongoing communications between the covered entity and BA regarding any updates or changes by the patient regarding the use and disclosure of their information or confidential communication requests (*see SHIPM Chapter 5, Confidential Communications*).
7. Ensure that its workforce complies with all applicable state and federal requirements and the BAA, MOU, or IA.
8. Ensure that any of the BA subcontractors that create, receive, maintain, or transmit health information on behalf of the BA, agree to the same restrictions and conditions that apply to the BA, including an executed BAA, MOU, or IA.
9. Report to the state entity any breaches or security incidents of health information within a specified timeframe to ensure the state entity is compliant with their reporting and notification requirements.
10. Make health information available for patients to access or incorporate any allowable amendments or addenda.
11. Make available the information required to provide an accounting of disclosures within a timeframe to ensure the covered entity is compliant with the 60 day response time requirement. *See SHIPM Chapter 5, Accounting of Disclosures*. *[45 C.F.R. § 164.528(c)]*
12. Comply with the requirements in the same manner as the state entity in carrying out the obligations related to the assigned responsibilities.
13. Make its internal practices, books, and records relating to the use and disclosure of health information received from, received by or created by the BA on behalf of the

state entity available to state and federal representatives for purposes of determining the state entity's and/or the BA's compliance with state and federal requirements.

14. Describe the conditions for termination of the BAA by the covered entity, specifically situations involving material breach by the BA including conditions for allowing the BA to cure the breach or end the violation.
15. At termination or expiration of the BAA, MOU, or IA, do either of the following:
    a. Return or destroy all health information received from, or created or received by the BA on behalf of the state entity that the BA still maintains in any form and retain no copies of such information, or
    a. If such return or destruction is not feasible, extend the protections of the BAA, MOU, or IA (contract) to the health information and limit further uses and disclosures to those purposes that make the return or destruction of the health information not feasible.

Consultation with your organization's legal counsel is recommended if this termination or expiration provision is inconsistent with the statutory obligations of the state entity or it's BA as this may support omitting this provision.

[45 C.F.R. § 164.504(e)(1), and § 164.504(e)(2); CA Civil Code § 56.10, § 1798.19, and § 1798.24; CA Health and Safety Code § 11845.5(c)(3)]

IV. References

45 C.F.R.

- § 164.308
- § 164.314
- § 164.502
- § 164.504
- § 164.528

CA Civil Code

- § 56.10
- § 1798.19
- § 1798.24

CA Health and Safety Code § 11845.5(c)(3)

CA SAM

- § 4983
- § 4983.1
- § 5305.8
- § 5310.3

NIST SP 800-53 Rev. 5

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Public Health Activities
SHIPM Chapter 2 – Required by Law and Required Disclosures
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 2 – De-identification
SHIPM Chapter 2 – Minimum Necessary
SHIPM Chapter 3 – Security
SHIPM Chapter 5 – Accounting of Disclosures
SHIPM Chapter 5 – Confidential Communications

VI. Attachments

Yes:
A – HIPAA Business Associate Agreement (template)
B – Guidance on HIPAA and Resellers of Cloud Computing Services

Chapter: 4 – Administrative		
Section: 4.4.0 – Business Associates		
4.4.2 – Oversight of Business Associates		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: Yes

I. Purpose

To provide guidance regarding the requirement that covered state entities conduct contractual compliance oversight on their business associates (BAs).

II. Policy

State entities are responsible to conduct oversight of all BAs to verify that they comply with requirements outlined in their business associate agreements (BAA).

Note - For governmental entities: This includes memoranda of understanding (MOU) that act as BAAs.
[45 C.F.R. § 164.504(e)(1)(ii); CA Health and Safety Code §§ 130300 – 130315]

III. Implementation Specifics

State entities are responsible to conduct oversight of their BAs to verify compliance with the patient privacy and security requirements in their BAAs - *see SHIPM Chapter 4, Business Associate Agreement.*

A. Oversight by State Entities. State entities are responsible to develop a program to ensure that their BAs are complying with all state and federal requirements in BAAs. *Note – oversight activities should ensure compliance of requirements associated with the BAA and not direction on how the BA performs their day-to-day operations or activities associated with the BAA.*

B. Demonstration of Compliance with BAAs. State entities must demonstrate through documentation (such as: protocols, procedures, communication logs, policies, emails, etc.) that they have implemented the following internal control requirements:

1. All patient requests regarding confidential communications and patient restrictions on use and disclosure must be communicated to the BA within two (2) business days.
2. Creation/maintenance of a list or log of all BAA contracts to include the name of the BA, start and end dates associated with the BAA, contract modifications and contact information for the BA.

3. Any risks from BA relationships must be evaluated and included in the state entity's risk analysis.
4. BA adherence with privacy and security protocols required by law, SHIPM, and the BAA must be verified and documented periodically. The frequency of this verification should be based on the results of the state entity's own risk analysis. Suggested factors to consider in the risk analysis might be the number and size of BAs, method and type of health information accessed by the BA, length of the relationships, etc.
5. Provide the BA with a means to notify the state covered entity if and when any violation of law, policy, or contract occurs, including any breaches or security incidents. Although the BAA requires the state entity be notified without unreasonable delay, best practices suggest notification occur no later than 24 – 48 hours after detection.
   [45 C.F.R. § 164.410, § 164.524, § 164.526, and § 164.528]
6. Procedures to take to ensure that if the state entity becomes aware of any pattern or practice that constitutes a violation of law and/or the BA's obligations under contract, the state entity takes reasonable steps to mitigate the defect or to end the business relationship. Reasonable steps will vary with the circumstances and nature of the BA relationship.

[45 C.F.R. § 164.308, § 164.314, § 164.410, § 164.524, § 164.526, and § 164.528; CA Civil Code §§ 56.01 – 56.99, and §§ 1798 – 1798.77, CA Health and Safety Code §§ 123111 – 123149.5]

IV. References

45 C.F.R.

- § 164.308
- § 164.314
- § 164.410
- § 164.504
- § 164.524
- § 164.526
- § 164.528

CA Civil Code

- §§ 56.01 – 56.99
- §§ 1798 – 1798.77

CA Health and Safety Code

- §§ 123111 – 123149.5
- §§ 130303 – 130315

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Marketing
SHIPM Chapter 3 – Security Management Process
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Confidential Communication

VI. Attachments

Yes – Oversight of BAs – Guidance and Checklist

Chapter: 4 – Administrative		
Section: 4.5.0 – Identifiers		
4.5.1 – Provider, Employers Identifiers		
Review Date: 06/01/2020	Revision Date: 06/01/2020	Attachments: No

I. Purpose

To provide guidance regarding the use of established/adopted national identification numbers (identifiers) for health care providers and employers.

II. Policy

Health care providers, health care plans, and employers who file electronic claims and conduct related electronic transactions (electronic data interchange) of health information *must* use national identification numbers (identifiers).

[45 C.F.R. § 162.404, § 162.406(a), § 162.408, § 162.410, § 162.412(a), § 162.412(b), § 162.414, § 162.504, § 162.506, § 162.508, § 162.510, § 162.512, § 162.514, § 162.600, § 162.605, and § 162.610]

III. Implementation Specifics

A. State entities are responsible to know when they are required to use one of the national identification standards. HIPAA has established national identification numbers (identifiers) for different entities, for the following reasons:

1. National health care provider identifier (NPI). NPI is a standard identifier for hospitals, doctors, nursing homes, and other health care providers. It facilitates the filing of electronic claims, as well as other standard electronic transactions with public and private insurance programs. Providers obtain an NPI by requesting a number through CMS' National Plan and Provider Enumeration System (NOPPES).
   a. A health care plan or health care clearinghouse must use the NPI of any health care provider (or subpart(s), if applicable), on all standard electronic transactions where that health care provider's identifier is required

      [45 C.F.R. § 162.412(a), and § 162.414]
   b. A health care plan may not require a health care provider that has been assigned an NPI to obtain an additional NPI

      [45 C.F.R § 162.412(b)]

2. Employer identifier number. Adopts the existing employer identification number (EIN) assigned by the Internal Revenue Service for employers in the health care industry, as a unique employer identifier when conducting standard electronic transactions for health care plan enrollments/premium payments.
[45 C.F.R. § 162.600, § 162.605, § 162.610, and § 162.610(b)]

IV. References

45 C.F.R.

- § 162.404
- § 162.406(a)
- § 162.408
- § 162.410
- § 162.412(a)
- § 162.412(b)
- § 162.414
- § 162.504
- § 162.506
- § 162.508
- § 162.510
- § 162.512
- § 162.514
- § 162.600
- § 162.605
- § 162.610

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – De-identification
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.6.0 – Requirements for Specific Organizations		
4.6.1 – Contractors		
Review Date: 06/01/2016	Revision Date: 06/01/2016	Attachments: No

I. Purpose

To provide information regarding contractors' responsibilities to maintain the privacy and security of health information.

II. Policy

Contractors who perform work for a covered entity that involves the use or disclosure of health information, must comply with the same privacy and security requirements as the organization with which they contract.

III. Implementation Specifics

A. State entities that are business associates, health care clearinghouses, health care plans, health care providers or hybrid entities are responsible to do all of the following:

1. Ensure contractors comply with the same requirements and restrictions for health information that apply to the state entity
2. Account for breaches by its contractor(s)
3. Treat breaches by a contractor as if they were breaches by the state entity

[45 C.F.R. § 160.402(c), § 162.923(c)(2), § 164.314(b)(2)(iii), § 164.404(a)(2), § 164.501, and § 164.514(h)(2)(ii)(C)]

IV. References

45 C.F.R.

- § 160.402(c)
- § 162.923(c)(2)
- § 164.314(b)(2)(iii)
- § 164.404(a)(2)
- § 164.501
- § 164.514(h)(2)(ii)(C)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative Requirements
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.6.0 – Requirements for Specific Organizations		
4.6.2 – Health Care Clearinghouses		
Review Date: 06/01/2016	Revision Date: 06/01/2016	Attachments: No

I. Purpose

To provide guidance regarding the privacy and security requirements for health care clearinghouses.

II. Policy

Health care clearinghouses are defined as covered entities under HIPAA, and must comply with the privacy, security, and transactions and code sets obligations. Health care clearinghouses may have either of the following with a patient:

- A direct treatment relationship
- An indirect treatment relationship

[45 C.F.R. § 162.930, § 164.500(b), § 164.502(e), §§ 164.504(d) - (e), § 164.524, and § 164.526]

III. Implementation Specifics

A. Health care clearinghouses, that have a direct treatment relationship, must comply with all privacy and security requirements.

B. Health care clearinghouses, that have an indirect patient relationship, do not need to do any of the following:

1. Provide a Notice of Privacy Practices (NPP)
2. Provide patients access to their medical records
3. Provide an accounting of health information disclosures

When no direct patient relationship exists, a health care clearinghouse must only use or disclose health information as expressly stated in their business associate agreement (BAA).

[45 C.F.R. § 164.500(b), § 164.502(e), and § 164.504(e)]

C. Business associate agreements. BAAs must clearly state that the health care clearinghouse will comply with the privacy and security regulations of the covered entity *(see SHIPM Chapter 4, Business Associate Agreement*).

IV. References

45 C.F.R.

- § 162.930
- § 164.500(b)
- § 164.502(e)
- § 164.504(d) – (e)
- § 164.524
- § 164.526

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 2 – Breach and Breach Notification
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative Requirements
SHIPM Chapter 4 – Transactions and Code Sets (TCS)
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Notice of Privacy Practices
SHIPM Chapter 5 – Accounting of Disclosures

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.6.0 – Requirements for Specific Organizations		
4.6.3 – Health Information Organizations		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: Yes

I. Purpose

To explain how privacy, security and administrative requirements apply to health information organizations (HIOs).

II. Policy

HIOs must comply with all of the privacy, security and administrative requirements applicable to business associates (BAs) or a state entity when providing services involving health information.

In addition, a HIO must enter into a valid written contract or other written agreement with all of the entities, BAs and other organizations which will be participating with the HIO to use, disclose, move, or store health information for health information exchange purposes. *[42 U.S.C. § 17901, and § 17938; 45 C.F.R. § 160.103; CA Civil Code § 1798.19]*

III. Implementation Specifics

Health information exchange is necessary and beneficial within a standardized framework that protects the privacy of health information and the security of data being exchanged.

A. A state entity that is a HIO, or conducts business with a HIO, must comply with all of the SHIPM policies pertaining to the privacy, security, and administrative requirements involving health information, as well as its own policies and those of the Office of Information Security (OIS).

B. A HIO (including Regional Health Information Organizations, E-Prescribing Gateways, and any vendor that contracts with an entity to allow that entity to offer health information to patients as part of its electronic health record), regardless of whether the HIO is considered a covered entity or business associate, must enter into a written contract or other written agreement with the entities, for which it provides health information exchange services. *At a minimum*, the agreement must address:

   1. The responsibility of participating organizations to obtain appropriate authorization from the patient to allow health information exchange.
   2. The minimum requirements of a valid business associate agreement (BAA). (*See SHIPM Chapter 4, Business Associate Agreement)*

3. The scope of the health information organization's (HIO's) governance, services, and functions.
4. The uses and disclosures of health information the HIO and all participating entities are permitted or required to make as they create, receive, move, transmit, store, or maintain electronic health information.
5. The safeguards the HIO and all participating entities will implement to protect the privacy and security of the electronic health information.
   [42 U.S.C. § 17938; 45 C.F.R. § 164.308(b), § 164.314(a), §§ 164.502(e)(1) – (2), and § 164.504(e)]
6. In the context of its networked environment, the HIO may enter into a single, multi-party BAA with multiple entities or organizations participating in health information exchange with the HIO.

C. A HIO may participate in an organization made up of other HIOs and other participating organizations. Such participation requires the HIO to enter into a written contract or other written agreement with the multiple HIOs in the organization providing health information exchange services and their participating entities, BAs and other participating organizations. *At minimum*, the agreement must address the following:
   1. The responsibility of participating organizations to ensure appropriate authorization is obtained from the patient to allow health information exchange.
   2. The minimum requirements of an adequate BAA.
   3. The scope of the multi-HIO organization's governance, services and functions.
   4. The uses and disclosures of health information the multi-HIO organization and its participating HIOs and entities are permitted or required to make as they create receive, move, transmit, store, or maintain electronic health information.
   5. The safeguards the multi-HIO and its participating HIOs and other participating organizations will implement to protect the privacy and security of the electronic health information.
      [42 U.S.C. § 17938; 45 C.F.R. § 164.308(b), § 164.314(a), §§ 164.502(e)(1) – (2), and § 164.504(e)]
   6. In the context of a networked multi-HIO environment, the HIO is permitted to enter into a single, multi-party data use (and reciprocal support) agreement with the multiple HIOs, entities, business associates and other organizations participating in the exchange of health information through the multi-HIO. *See attached example of the California Data Use and Reciprocal Support Agreement (CalDURSA)*.

D. To help meet the goals set for health information exchange by the State of California and the federal Office of the National Coordinator for Health Information Technology, state entities that provide services as a health information organization or a multi-HIO organization are required to use the CalDURSA as its written agreement with participating organizations, or a written agreement with all the same elements as the CalDURSA.
[45 C.F.R. § 164.308(b), and §§ 164.502(e)(1) - (2); CA Civil Code § 56.10(a), and § 56.37(a)]

IV. References

42 U.S.C.

- § 17901
- § 17938

45 C.F.R.

- § 160.103
- § 164.308(b)
- § 164.314(a)
- §§ 164.502(e)(1) – (2)
- § 164.504(e)

CA Civil Code

- § 56.10(a)
- § 56.37(a)
- § 1798.19

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 - Privacy
SHIPM Chapter 2 – Health Information Exchange (HIE)
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative Requirements
SHIPM Chapter 4 – Business Associate Agreement
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

Yes - California Data Use and Reciprocal Support Agreement (CalDURSA), dated July 24, 2014.

Chapter: 4 – Administrative		
Section: 4.6.0 – Requirements for Specific Organizations		
4.6.4 – Pharmaceutical Companies		
Review Date: 06/01/2016	Revision Date: 06/01/2016	Attachments: No

I. Purpose

To explain that privacy, security, and administrative requirements apply to permitted communications from pharmaceutical companies to a patient.

II. Policy

Pharmaceutical companies that communicate with patients are required to protect the privacy and security of the patient's health information.

III. Implementation Specifics

State entities contracting with pharmaceutical companies are responsible to ensure refill reminders or communications about a drug or biologic currently prescribed for a patient, comply with both of the following:

1. The pharmaceutical company has a *current* direct treatment relationship, *and*
2. A current valid prescription

This type of communication is exempt from regulations regarding use of health information for marketing purposes. *[45 C.F.R. § 164.501]*

IV. References

45 C.F.R. § 164.501

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 3 – Security
SHIPM Chapter 4 – Administrative
SHIPM Chapter 5 – Patient Rights

VI. Attachments

None

Chapter: 4 – Administrative		
Section: 4.6.0 – Requirements for Specific Organizations		
4.6.5 – Hybrid Entities		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: No

I. Purpose

To provide guidance regarding requirements of state entities that self-designate as Hybrid Entities.

II. Policy

Policies and procedures must be implemented and maintained which outline the requirement for Hybrid Entities to create and maintain adequate "firewalls" or separation between covered and non-covered health care components within their organization.
[45 C.F.R. § 164.103, § 164.105, § 164.314, § 164.316, § 164.504, and § 164.530]

III. Implementation Specifics

State entities that are Hybrid Entities have business activities that include HIPAA covered functions and non-covered functions. Any patient health information collected and used by the covered function portion of the organization cannot be used or shared with the non-covered portion of the organization, even if a single employee has duties in both areas.

A. Written Declaration of Hybrid Entity Status. State entities must declare in writing that they are a Hybrid Entity and must declare which components/portions of their organization are covered under HIPAA. The designations must be in writing as part of the state entity's policies and procedures. It is recommended that the state entity also publish the designation on its website. The state entity must designate in writing all portions of the organization that meet the definition of covered entity and business associate.
[45 C.F.R § 164.105(a)(2)(iii)(D)]

B. Inventory and Location/Movement of Health Information. To ensure separation between covered and non-covered components, Hybrid Entities must:

1. Determine what health information and document the location of health information as well as where it moves within the organization at least once per year.
2. Assess which workforce members have roles that require them to have access to health information. Ensure those workforce members do indeed work in areas the organization has designated as covered.

3. Train all workforce members in the covered portions of the organization, to prevent access by staff of non-covered portions.

C. Implement and Maintain Policies and Procedures. State entities that are Hybrid Entities must implement and maintain policies and procedures outlining the specific methods by which they will protect patient health information within their organizations, including methods to inventory the location and movement of protected health information and how they will separate covered and non-covered components.

D. Separation between Covered and Non-Covered Components. State entities must create an adequate "firewall" and separation between covered and non-covered health care components within the organization in that patient health information that is collected and used by the covered component may not be disclosed to or used by the non-covered component. To satisfy this, the following are required:

1. Health information stored in the covered portion of an organization cannot be available or viewable by workforce members in the non-covered portion of the organization.
2. If a single workforce member has duties in both covered and non-covered portions of the organization, they cannot use the health information they obtain during their duties in the covered portion of the organization for their duties in the non-covered portion.
3. Documentation of who is designated to have access to what health information and for what purpose must be maintained for six (6) years.
   [45 C.F.R § 164.105(c)]

E. Any risks associated with the separation of covered and non-covered components of the organization and the movement of protected health information between these components must be considered and documented in the organization's risk analysis.

IV. References

45 C.F.R.

- § 164.103
- § 164.105
- § 164.314
- § 164.316
- § 164.504
- § 164.530

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 4 – Business Associate Agreement

VI. Attachments

None

Chapter 5 – Patient Rights

Chapter: 5 – Patient Rights		
Section: 5.1.0 – Accounting of Disclosures		
5.1.1 – Accounting of Disclosures		
Review Date: 06/01/2018	Revision Date: 06/01/2018	Attachments: No

I. Purpose

To provide guidance regarding the requirements for tracking disclosures of health information and the patient's right to request and receive an accounting of those disclosures.

II. Policy

Disclosures of health information must be documented and tracked in order to provide an accounting of such disclosures to the patient upon the patient's request.
[45 C.F.R. § 164.528; CA Civil Code § 1798.25; Eisenhower Medical Center v. Superior Court, 226 Cal.App.4th 430 (2014)]

For accounting of disclosures information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

A. State entities are responsible to create, implement, and maintain policies and procedures stating how to process and document disclosures of health information as well as patient requests for an accounting of disclosure.

B. State entities are responsible to document, track and maintain information concerning disclosures of health information. This tracking must document what, when, why and to whom disclosures are made.

C. State entities that are health care plans, health care providers or hybrid entities are responsible to provide the patient with an accounting of the disclosures of their health information.

The accounting must include disclosures made by the state entity as well as any disclosures made to or by any business associates (BAs) of the state entity.
[45 C.F.R. § 164.528(b)(1)]

1. Timing of response to an accounting of disclosure request. State entities are responsible to respond to a request for an accounting of disclosures no later than 60 days after receipt of such a request.

   If unable to respond within this period of time, the state entity may extend the time by no more than 30 days provided that, within the initial 60 day period, the state entity provides the patient with a written statement of the reasons for the delay and the date by which the accounting will be provided. Only one (1) 30-day extension is permitted.

   [45 C.F.R. § 164.528(c)(1)]

2. Content of disclosures accounting. The accounting for each disclosure of health information must include all of the following:
   a. The date(s) of the disclosure(s)
   b. The name and title of the entity or person to whom the information was provided, and their recorded address
   c. A brief description of the health information disclosed
   d. A brief statement describing the reason for the required or permitted disclosure (e.g., pursuant to a subpoena), or a copy of the written request if applicable

   [45 C.F.R. § 164.528(b)(2); CA Civil Code § 1798.25]

   Special Note: Subsequent patient requests for accounting of disclosures, within 12 months of the first accounting of disclosure, need only include any incremental disclosures made since the original accounting.

3. Charge for the accounting.
   a. The first accounting of disclosures made to a patient during any 12-month period of time must be provided free of charge
   b. For any subsequent request for an accounting of disclosures made by the same patient made within this 12-month period, the state entity may impose a reasonable, cost-based fee for the accounting, provided that the patient is informed in advance of the fees that will be charged and provides the patient with an opportunity to withdraw or modify the request for a subsequent accounting to avoid or reduce the fee

   [45 C.F.R. § 164.528(c)(2)]

D. Exceptions to required disclosure accounting. The following types of disclosures are excluded from the accounting of disclosures requirement (*see section V. Related Policies – below*):
   1. Disclosures made for treatment, payment**,** and health care operations
   2. Disclosures made to the patient about themselves

3. Disclosures resulting from or incident to otherwise permitted disclosure
4. Disclosures made pursuant to an authorization
5. Disclosures made for a facility's directory, or to persons involved in the patient's care or for related purposes
6. Disclosures that are part of a limited data set

[45 C.F.R. § 164.528(a)(1)]

E. Disclosure accounting for research purposes. If during the period of time covered by the requested accounting, the state entity makes disclosures for specific research purposes regarding 50 or more individuals' records, the state entity may account for the disclosures by providing all of the following:

1. The name of the protocol or other research activity
2. A plain language description of the research protocol or activity, including the purpose of the research and the criteria for selecting certain records
3. A brief description of the type of health information that was disclosed
4. The dates or periods of time during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the accounting period
5. The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed
6. A statement that the health information may or may not have been disclosed for a particular protocol or particular research activity

If it is reasonably likely that the health information was disclosed for a research protocol or activity, the state entity shall, if requested by the patient, assist the patient in contacting the entity that sponsored the research and the researcher.

[45 C.F.R. § 164.528(b)(4)]

F. Documentation. The state entity shall maintain a written, including electronic, record of each accounting of disclosures sufficient to demonstrate compliance with requirements. At a minimum, this must include documentation of the information required to be included in each accounting, and the titles of persons or offices responsible for receiving and processing requests for accounting of disclosures. Documentation must be retained for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

[45 C.F.R. § 164.528(d), and § 164.530(j)]

The state entity Business Associate Agreement (BAA) needs to include a requirement that all BAs document, track and account for all disclosures required to comply with an accounting of disclosures. In addition, the BAA should address how and when (timeframe) the BA is to provide the state entity with the information necessary to comply with an accounting when requested by the patient.

IV. References

45 C.F.R.

- § 164.528
- § 164.530(j)

CA Civil Code § 1798.25

Case Law - Eisenhower Medical Center v. Superior Court, 226 Cal.App.4th 430 (2014)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Privacy
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Health Oversight
SHIPM Chapter 2 – Law Enforcement
SHIPM Chapter 2 – Opportunity to Agree or Object
SHIPM Chapter 2 – Research
SHIPM Chapter 2 – Victims of Abuse, Neglect, or Domestic Violence
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – De-identification

VI. Attachments

None

Chapter: 5 – Patient Rights		
Section: 5.2.0 – Amendments		
5.2.1 – Patient's (Individual's) Right to Amend Medical Records		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding patient requests for changes or corrections (amendments) to their medical records.

II. Policy

Patients or patient representatives may request any portion of the patient's medical record be changed, corrected, or amended by submitting a 250 word maximum addendum of additions or corrections to the medical record. The addendum must be kept and distributed with the record for as long as the covered entity, health care provider, health care plan, or health care clearinghouse maintains the records.

A state entity must either make the requested amendment or notify the requestor that the request has been denied within 30 days of the request.
[45 C.F.R § 164.501, and § 164.526; CA Civil Code § 1798.35; CA Health and Safety Code § 123111(a); CA SAM § 5310.4]

For patient's right to amend medical records information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

A. State entities are responsible to create, implement, and maintain policies and procedures stating how to process and document patient requests for amendment to their medical records.
[45 C.F.R. § 164.530(i)]

1. Patient amendment requests must be in writing.
2. State entities are responsible to advise their patients in advance of this requirement by including a statement in the Notice of Privacy Practices *(see SHIPM Chapter 5, Notice of Privacy Practices).*

3. Correspondence regarding patient requests for amendment, and relating to denial or acceptance of requests to amend, should be filed in the patient's medical record and appended to the information in question; as well as be accessible and available to staff in designated areas.
4. Initial patient amendment requests. State entities have 30 days to do either of the following:
   a. Amend the patient's medical records, or
   b. Deny the patient's request in whole or part
5. Response to appeal of denial. State entities must respond to the patient within either of the following:
   a. Within 30 days of receipt of the denial appeal, or
   b. Notify the patient that the appeal may take another 30 days (for a total of no more than 60 days) from receipt of the denial appeal

   [45 C.F.R. §§ 164.526(b)(1), (c)(1); CA Civil Code §§ 1798.35 - 1798.36; CA Health and Safety Code § 123111]

B. Acceptance of request for amendment. When a correction is made, state entities are responsible to make reasonable efforts to provide the corrected information to its business associates (BAs) and others who are known to have the health information that was amended.
[45 C.F.R § 164.526(c)(3); CA Civil Code § 1798.35]

If the state entity accepts the requested amendment, in whole or in part, at a minimum the policies and procedures must address all the following:

1. The state entity should place a copy of the amendment in the patient's medical record appended to the original documentation, with a clear indication that the original has been amended and the date of the amendment.
2. The state entity should also ensure that the amended documents are placed appropriately in the patient's electronic health record when one exists.
3. The state entity should notify the relevant persons with whom the amendment needs to be shared, as identified by the patient on the original amendment request. If the patient is unsure as to who should receive the amended information, the state entity should work with the patient to ensure that all parties are appropriately identified.
4. The state entity must identify other persons, including BAs, that are known to have the patient's health information and that may have or may rely on it.
5. State entities are responsible to inform the patient in writing that the amendment has been accepted.

If only a portion of the amendment has been accepted, the entity must also notify the patient that a portion has been accepted and a portion denied. The portion denied must follow the same procedures as documented in *Section D below*.

[45 C.F.R. § 164.526; CA Civil Code § 1798.35(a); CA Health and Safety Code § 123111(b)]

C. Denial of request for amendment. A state entity may deny a patient's request for amendment, for any of the following reasons, if it determines that the health information or record that is the subject of the request:

1. Was not created by the state entity, unless the patient explains that the originator of health information is no longer available.
2. Would not be available for inspection.
3. Is accurate and complete.

[45 C.F.R § 164.526(a)(2)]

D. Content of the denial. The denial, in whole or in part, should be written in plain language and at a minimum must address all of the following:

1. The reason for the refusal.
2. A description of how the patient can request a review by the head of the state entity, or an official specifically designated by the head of the state entity.

   The reviewer cannot be the same person who denied the patient's request initially.
3. The name, title, and business address of the reviewing official.
4. A notice that the patient has a right to submit a written statement disagreeing with the denial with an explanation of how the patient may file such a statement.
5. A notice that, if the patient does not submit a statement of disagreement, the patient may request that any future disclosures of the disputed health information include the request for amendment and the denial.
6. A description of how the patient may file a complaint with the state entity or to the Secretary of the U.S. Department of Health and Human Services (HHS). The description must include the name or title and telephone number of the contact person for the complaint.
7. If the patient submits a written statement of disagreement:
   a. The state entity may prepare a written rebuttal and is responsible to provide a copy of the written rebuttal to the patient.
   b. The statement of disagreement must be included in any future disclosure of the health information with a clear indication of which portion of the medical record is disputed.

[45 C.F.R. §§ 164.526(d)(1) – (d)(5); CA Civil Code §§ 1798.35 – 1798.37]

E. Documentation. All the following documentation must be appended (or otherwise linked) to the health information that is the subject of the disputed amendment and must be kept for six (6) years:

1. The patient's request for amendment
2. The organization's amendment denial letter
3. The patient's statement of disagreement, if any
4. The organization's written rebuttal, if any

[45 C.F.R § 164.526(d)(4), and § 164.530]

IV. References

45 C.F.R.

- § 164.501
- § 164.526
- § 164.530

CA Civil Code §§ 1798.35 – 1789.37

CA Health and Safety Code § 123111

CA SAM § 5310.4

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Opportunity to Agree or Object
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Patient's (Personal) Representatives
SHIPM Chapter 5 – Patient's (Individual's) Right to Access Health Information
SHIPM Chapter 5 – Notice of Privacy Practices

VI. Attachments

None

Chapter: 5 – Patient Rights		
Section: 5.3.0 – Notice of Privacy Practices		
5.3.1 – Notice of Privacy Practices		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: Yes

I. Purpose

To ensure that all patients are informed about state and federal requirements regarding their right to know how their health information will be used and disclosed, and the actual privacy practices of the entities.

II. Policy

A Notice of Privacy Practices (NPP), which reflects the actual privacy practices of the entity, must be given to patients and must include all the following:

- The uses and disclosures of health information that may be made
- The patient's rights and how to exercise them
- The entities' legal duties to maintain privacy of health information

All state entities that provide health care must comply with this policy.
[45 C.F.R. § 164.520; CA SAM § 5310.1]

III. Implementation Specifics

A. Contents of the Notice of Privacy Practices. A complete list of the required components can be found in *Attachment A – Model Notice of Privacy Practices*.

To validate that the NPP has the required components, see *Attachment B – Notice of Privacy Practices – Checklist.*
[45 C.F.R. § 164.520(b)(1)]

B. Distribution of NPP to patients by health care providers.

1. Health care providers with a direct treatment relationship (e.g., face-to-face treatment, telemedicine or telehealth interactions and phone consults) must:
   a. Ensure the NPP is provided to the patient no later than the date of the first service delivery. If the first service is delivered electronically, the provider must send the NPP electronically, close to the time of service.
   b. In an emergency situation, the NPP may be provided as soon as possible.
   c. Post the NPP in a clear and visible location, such as waiting rooms and registration areas, where patients can read the notice.

d. Prominently post the NPP, so that it stands out, on any website that the provider maintains containing information about the provider's services. Also make the NPP available electronically through the website.

e. Whenever updated, make the revised NPP available upon request and post the revised version in the facility and on the facility's website.

2. Health care providers with an indirect treatment relationship (e.g., laboratories, pharmacies) are only required to produce the NPP upon request.

[45 C.F.R. § 164.520(c)(1)]

C. Distribution of NPP to patients by health care plans. Health care plans must provide an NPP:

1. To patients then covered by the plan - if not provided by the initial 2003 compliance date, you must provide it immediately,
2. To patients who are new enrollees, at the time of enrollment, *and*
3. To patients covered by the plan within 60 days of a material revision to the NPP (e.g., change in practices, law or uses and disclosures) or prominently post on its website the change or providing a revised NPP by the effective date of the material change. In its next annual mailing to patients covered by the plan, the health plan must also provide the revised NPP, or information about the material change and how to obtain the revised NPP.
4. To the named insured of the policy at least once every three (3) years and notify the patients covered by the plan of the ongoing availability of the NPP and how to obtain a copy.

[45 C.F.R. § 164.520(c)(2)]

D. Patient acknowledgment. Health care providers must make a good faith effort to obtain a written acknowledgment that the patient received the provider's NPP. Except in emergency treatment situations, providers are also required to document good faith efforts to obtain the acknowledgment, including addressing situations where a patient refuses to sign an acknowledgment. A model acknowledgment form can be found in *Attachment C – Notice of Privacy Practices – Acknowledgment of Receipt.*

[45 C.F.R. § 164.520(c)(2)(ii)]

E. Health information must not be used or disclosed in any manner inconsistent with the NPP.

[45 C.F.R. § 164.502(i)]

F. Incidental uses and disclosures. There are certain incidental uses or disclosures of health information that may occur while providing services or conducting business. Reasonable efforts to limit these incidental uses and disclosures must be referenced in the NPP.

G. Exceptions. Health care providers are not required to distribute the NPP to inmates. See *Attachment D – Notice of Privacy Practices – FAQ* section on inmates.
[45 C.F.R. § 164.520(a)(3)]

H. Translation in other languages. The NPP should be translated and made available in all languages, other than English, consistent with applicable State and federal requirements to ensure effective communication.

I. The NPP should state that the facility / agency / department does not discriminate on the basis of race, color, national origin, sex, age, or disability.
[Patient Protection and Affordable Care Act, 42 U.S.C. § 1557]

J. Documentation requirements. NPPs, and if applicable, any written acknowledgment of receipt of the notice or documentation of good faith efforts shall be kept for a minimum of six (6) years from the later of the creation of the notice or the date the notice was last in effect.
[45 C.F.R. § 164.520(e)]

IV. References

Patient Protection and Affordable Care Act, 42 U.S.C. § 1557
45 C.F.R.

- § 164.502(i)
- § 164.520

CA SAM § 5310.1

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Incidental Disclosure

VI. Attachments

Yes:

A – Model Template Notice of Privacy Practices
B – Notice of Privacy Practices – Checklist
C – Notice of Privacy Practices – Acknowledgment of Receipt
D – Notice of Privacy Practices - FAQ

Chapter: 5 – Patient Rights		
Section: 5.4.0 – Patient Rights - Access		
5.4.1 – Patient's (Individual's) Right to Access Health Information		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

I. Purpose

To provide guidance regarding patients' rights, and limitations, to access their health information.

II. Policy

Patients have the right to inspect, review, and obtain a copy of their health information held by covered entities, business associates (BAs), health care clearinghouses, health care plans, health care providers, and hybrid entities, with a few exceptions listed below.
[45 C.F.R. § 164.504(e)(2)(ii)(E), § 164.504(f)(2)(ii)(E), and § 164.524; CA SAM § 5310.4]

For information about a patient's right to access health information related to specially protected information (Genetic information, HIV/AIDS related information, Mental Health records, Substance Use Disorder treatment records, Developmental Service records and Psychotherapy notes are types of Specially Protected Health Information) - *see SHIPM Chapter 2, Specially Protected Information.*

III. Implementation Specifics

With a few exceptions, state entities that are covered entities, BAs, health care clearinghouses, health care plans, health care providers, or hybrid entities have the responsibility to provide access to the health information they maintain in the designated record set, upon patients' request.

- For organizations with a designated record set, patient access is limited to the health information defined in the designated record set for as long as the health information is maintained in the designated record set.
- For organizations without a designated record set, patient access is allowed for all health information in the possession of the organization, with the exception of specially protected health information covered by policies found in *SHIPM Chapter 2, Specially Protected Information* (for example, Psychotherapy Notes).

[45 C.F.R. § 164.524; CA Civil Code § 1798.34; CA Health and Safety Code § 123110]

A. State entities must provide health information access to the following:

1. Patients.

   a. Patient requesting health information access. Except as otherwise provided in this SHIPM policy, individuals have the right to request access to inspect and obtain a copy of their health information.

   b. Minor patients. State entities shall allow a patient, who is a minor, to inspect or obtain copies of health information pertaining only to health care of a type for which the minor is lawfully authorized to consent.

   [45 C.F.R. § 164.502(g)(3); CA Health and Safety Code § 123110]

2. Release of information. Patients may designate another person (including a patient representative) to whom the state entity must provide access to the patient's health information.
   [45 C.F.R. § 164.524(c)(3)(ii); CA Civil Code § 56.10(b)(9)]

3. Patient representatives. For access purposes, patient representatives are treated in the same manner as the patient who is the subject of the health information.
   [45 C.F.R. § 164.502(g)(1); CA Health and Safety Code § 123110]

   a. Minor patients. The patient representative of a minor shall not be entitled to inspect or obtain copies of the minor health information in the following scenarios:

      i. When the minor patient has a right to inspect or obtain copies.
      [CA Health and Safety Code § 123110]

      ii. If the health care provider determines that access to the health information, requested by the patient's representative, would have a detrimental effect on the provider's professional relationship with the minor patient, or the minor's physical safety or psychological well-being.
      [45 C.F.R. § 164.502(g)(3)(ii)(B); CA Health and Safety Code § 123115]

      iii. If a psychotherapist knows that the minor patient has been removed from the physical custody of his or her parent or guardian.

      This restriction shall not apply, if the juvenile court has issued an order authorizing the parent or guardian to inspect or obtain copies of the mental health information of the minor patient, after finding that such an order would not be detrimental to the minor patient.
      [45 C.F.R. § 164.502(g)(3)(ii)(B); CA Health and Safety Code § 123116]

   b. State entities may elect not to treat an individual as the patient's representative if there is a reasonable belief that:

      i. The patient has been, or may be subject to domestic violence, abuse, or neglect by the individual

ii. Treating such individual as the patient's representative could endanger the patient

iii. The state entity, in the exercise of their expert knowledge and opinion, decides that it is not in the best interest of the patient to treat the individual as the patient's representative

[45 C.F.R. § 164.502(g)(5)]

B. Prescribed Timeframes. Upon receiving a request to access, inspect, or receive a copy of the designated record set, the state entity is responsible to process the request within the following timeframes:

1. To provide copies of health information, related to health history, diagnosis, condition of the patient, or to treatment provided, or to billing records and other elements of the designated record set within 30 days.
   [45 C.F.R. § 164.524; CA Civil Code § 1798.34(a); CA Health and Safety Code § 123140]
2. To provide a copy of the portion of the health records necessary to support an appeal or claim regarding eligibility for public benefits (e.g., Medi-Cal, Social Security disability insurance benefits, Supplemental Security Income, State Supplementary Program for the Aged, Blind, and Disabled, In-Home Supportive Services, CalWORKS, federal veterans service-connected compensation and non-service connected pension disability benefits and CalFRESH), a petition for U nonimmigrant status under the Victims of Trafficking and Violence Protection Act, or a self-petition for lawful permanent residency under the Violence Against Women Act within 30 days.
   [45 C.F.R. § 164.524(c)(4); CA Civil Code § 1798.34(a); CA Health and Safety Code § 123110(d) and (f), and § 123114]
3. To provide copies of health information within 15 days following patient's inspection of records.
   [CA Civil Code § 1798.34(b)]
4. To advise the patient in writing within 60 days where to direct their request for access, if the state entity does not maintain the designated record set (*if the state entity knows where the requested health information is maintained by the BA or third party)*

[45 C.F.R. §§ 164.524]

C. Obtain information in the format they choose. If it is reasonable to do so, the state entity must provide the health information in the format requested by the patient (such as a readable hard copy or in some other form) that can be agreed upon by the state entity and the patient.
[45 C.F.R. § 164.524(c)(2)]

1. The state entity may not deny access or refuse to provide copies of the health information based on a disagreement as to format
2. If the state entity maintains the health information in an electronic health record, the state entity must provide the patient with an electronic copy of that health information, if the patient chooses

D. The state entity must ensure fees charged are reasonable or allowed.

1. For requests for health information to support an appeal or claim regarding eligibility for a public benefit program (e.g., Medi-Cal, Social Security disability insurance, Supplemental Security Income, or State Supplementary Program for the Aged, Blind and Disabled), a petition for U nonimmigrant status under the Victims of Trafficking and Violence Protection Act, or a self-petition for lawful permanent residency under the Violence Against Women Act patients are entitled to receive one copy free of charge provided that the patient makes the request in writing and provides proof that health information is needed.
   [45 C.F.R. § 164.524(c)(4); CA Health and Safety Code § 123110(d) and (f), and § 123114]
2. Foster Youth have the right to review and received copies of their medical records to the extent they have the right to consent to the treatment provided in the medical record, at no cost until they are 26 years of age.
   [CA Welfare and Institutions Code § 16001.9(a)(22)(B)]
3. Reasonable, cost-based fees may not exceed ten (10) cents ($.10) per page – fees can only include the cost of:
   a. Labor for copying PHI (paper or electronic)
   b. Supplies to create paper copy or electronic media (if electronic copy is to be provided on portable media)
   c. Postage
   d. Preparing an explanation or summary of PHI (if requested and agreed to by requestor)
      [45 C.F.R. § 164.524(c)(4); CA Civil Code § 1798.33; CA Health and Safety Code § 123140]

E. Exceptions to granting access.

1. State entities can deny patients access to their health information for the following reasons:
   a. The state entity does not have the patient's health information. If this is the case, the state entity must notify the patient in writing that it does not maintain the patient's health information.

b. Health information compiled in anticipation of or use in a civil, criminal, or administrative action or proceeding. *(State entities are encouraged to discuss each request with their legal counsel)*.
[45 C.F.R. § 164.524(a)(1)(ii)]

c. Certain state entities may deny a patient access without providing the patient an opportunity for review when the health information that was obtained from a family member, not in the role of a health care provider, under a promise of confidentiality and the access requested would likely identify the source. This applies only to records related to alcohol and other drug abuse treatment programs licensed by the Department of Health Care Services (DHCS); information on consumers from Department of Developmental Services (DDS); and information on patients at Department of State Hospitals (DSH) facilities. These protections follow the health information when transferred between state entities. *(State entities should consult with their legal counsel.)*
[45 C.F.R. § 164.524(a)(2)(v); CA Health and Safety Code § 11845.5(c)(4); CA Welfare and Institutions Code §§ 4514(d), and § 5328(a)(4)]

d. A state entity may deny a patient access to mental health records (MHR) if the patient is given the right to have denials reviewed under the following circumstances:
   i. A licensed health care professional determined that access could endanger the life or physical safety of the patient or another person
   [45 C.F.R. § 164.524(a)(3)(i) and (iii); CA Civil Code § 1798.40(f); CA Health and Safety Code § 123115(b)]
   ii. The request is made by the patients' representative, and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the patient or another person
   [45 C.F.R. § 164.524(a)(3)(iii); CA Civil Code § 1798.40(f); CA Health and Safety Code § 123115(b)]

e. When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records (MHRs) requested, the provider may decline to permit inspection or provide copies of the MHRs to the patient, subject to all the following conditions:
   i. The health care provider shall make a written record, to be included with the MHRs requested, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the MHRs, including a description of the specific adverse or

detrimental consequences to the patient that the provider anticipates would occur if inspection or copying were permitted

ii. The health care provider shall permit inspection by, or provide copies of the MHRs to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor, designated by request of the patient. The health care provider shall indicate the request was made in the MHR of the patient

iii. The health care provider shall inform the patient of the provider's refusal to permit inspection or receipt of copies of the requested MHRs, explain how to make a complaint, and inform the patient of the right to require the provider to permit inspection by, or provide copies to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor designated by written authorization of the patient

[45 C.F.R. § 164.524(d)(2); CA Health and Safety Code § 123115(b)]

2. State entities shall not deny access, or refuse to provide copies, because of an unpaid bill for health care services.
[CA Health and Safety Code § 123110(j)]

3. If access is denied, the state entity must:

   a. Provide a written denial in plain language to the patient that includes all of the following:

      i. The basis for the denial

      ii. An explanation of the patient's review rights

      iii. A description of how the patient may request a review of the denial, including the name or title, and telephone number of the state entity's Privacy Official designated to receive complaints or requests for review

   b. State entities are responsible to designate a licensed health care professional to act as the reviewing official. The reviewing official may not have participated in the denial of access decision and must provide a written decision to the patient within a reasonable time period.
   [45 C.F.R. § 164.524(a)(4), and § 164.524(d)(4)]

F. Administrative responsibilities. State entities that are covered entities, business associates, health care clearinghouses, health care providers, health care plans, or hybrid entities have the following administrative responsibilities regarding health information access requests:

1. Policy and Procedure. State entities are responsible to implement policies and procedures for:
   a. Providing access for the patient (or patient representative) to the patient's health information
   b. What is included in the designated record sets, and that patients may access the designated record sets
   c. The titles of the persons or offices responsible for receiving and processing patient requests for access
   d. Non-discrimination in the transmittal of x-rays or other patient records. A health care provider may establish reasonable conditions, including a reasonable deposit fee, to ensure the return of the original x-rays transmitted to another health care provider, provided the conditions do not discriminate on the basis of, or in a manner related to, the license of the provider to which the x-rays are transmitted

   [45 C.F.R. § 164.524(e), and § 164.530(i); CA Health and Safety Code § 123110 – 123149.5]
2. Include in Notice of Privacy Practices (NPP). The NPP must provide information that describes how a patient can request access in writing to health information, and how to request a review of denial of access.
   [45 C.F.R. § 164.520(b)(iv)(C), and § 164.524)]
3. Verify identity. State entities are responsible to require reasonable verification of identification prior to permitting inspection or copying of patient records. This requirement shall not be used oppressively or discriminatorily to hinder or delay compliance with these provisions (*see SHIPM Chapter 3, Verification of Identity*).
4. Document Retention. Documentation relating to requests for access must be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.
   [45 C.F.R § 164.530(d)]

IV. References

45 C.F.R.

- § 160.306
- § 164.502(g)(1)
- § 164.502(g)(3)
- § 164.502(g)(5)
- § 164.504(e)(2)(ii)(E)
- § 164.504(f)(2)(ii)(E)
- § 164.520(b)(iv)(C)

- § 164.524
- § 164.530

CA Civil Code

- §§ 56 – 56.34
- §§ 1798.24 – 1798.44

CA Health and Safety Code

- § 11845.5(c)(4)
- §§ 123110 – 123149.5

CA Welfare and Institutions Code

- § 4514(d)
- § 5328(a)(4)
- § 16001.9(a)(22)(B)

CA SAM § 5310.4

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Patient's (Personal) Representative
SHIPM Chapter 3 – Verification of Identity
SHIPM Chapter 5 – Patient's (Individual's) Right to Amend Medical Records
SHIPM Chapter 5 – Notice of Privacy Practices
SHIPM Chapter 5 – Confidential Communication

VI. Attachments

None

Chapter: 5 – Patient Rights		
Section: 5.5.0 – Restrictions		
5.5.1 – Restriction for Self-Pay		
Review Date: 06/01/2019	Revision Date: 06/01/2019	Attachments: No

I. Purpose

To provide guidance regarding the requirements to address a patient's right to restrict disclosure of their health information when they have self-paid for services.

II. Policy

Patients have the right to restrict the use and disclosure of their own health information when the services have been self-paid.

III. Implementation Specifics

A. State entities are responsible to comply with a patient's request that health information not be disclosed to a health care plan for payment or health care operations *only* if the health information is related to services that have been paid out-of-pocket in full, either by the patient, or by another person on the patient's behalf.
[45 C.F.R. § 164.522(a)]

1. A state entity *must* honor the patient's restriction request *if* either are met:
   a. The disclosure is for the purpose of carrying out payment or health care operations
   b. The disclosure is not otherwise required by law
   [45 C.F.R § 164.510(b), and § 164.522(a)]
2. Restriction requests should be in writing. If the patient cannot or will not submit the request in writing, the workforce member receiving the request should document the request in writing.
3. A state entity is not obligated to restrict the use of health information under any of the following circumstances:
   a. If the patient was informed in advance and had the opportunity to agree, object, or restrict the sharing of health information
   [45 C.F.R. § 164.510]
   b. When an authorization is not required
   [45 C.F.R. § 164.512]

4. Denial of restriction request. A state entity can deny the requested restriction if the request is related to services that were not paid for in full by the patient or on the patient's behalf.
   [45 C.F.R. § 164.522(a)]
5. Exceptions to restricted use and disclosure of health information. Exceptions include psychotherapy notes, information compiled for use in civil, criminal or administrative actions, and information that is subject to prohibition by the Clinical Laboratory Improvements Amendments.

   Consult with your organization's legal counsel prior to developing or implementing operational policies and procedures to comply with this section of the implementation specifics.
   [42 C.F.R. § 493, 45 C.F.R. § 164.520(a), and § 164.522(a)]
6. Termination of restriction. A state entity may terminate a restriction *if* either of the following occurs:
   a. The patient requests the termination in writing, or
   b. The patient agrees to or requests the termination orally and a workforce member documents the request
   [45 C.F.R. § 164.522]

B. Documentation. State entities are responsible to do all the following:
1. Document all requests for health information use or disclosure restriction
2. Document the reason for a denial of request for restriction
3. Maintain correspondence and associated documentation related to patient requests for restriction, including denials, in the patient's medical record, in accordance with the records retention policy (*for a minimum of six (6) years)*

[45 C.F.R. § 164.522(b), and § 164.530(j)]

IV. References

42 C.F.R. § 493

45 C.F.R.

- § 164.510
- § 164.512
- § 164.520(a)
- § 164.522
- § 164.530(j)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 2 – Authorizations
SHIPM Chapter 2 – Specially Protected Information
SHIPM Chapter 2 – Opportunity to Agree or Object
SHIPM Chapter 4 – Business Associate Agreement

VI. Attachments

None

Chapter: 5 – Patient Rights		
Section: 5.5.0 – Restrictions		
5.5.2 – Confidential Communication		
Review Date: 06/01/2017	Revision Date: 06/01/2017	Attachments: No

I. Purpose

To provide guidance regarding the obligation to address a patient's request to receive confidential communications.

II. Policy

Patients have a right to request to receive communications by alternative means or at alternative locations.
[45 C.F.R. § 164.522(b)]

III. Implementation Specifics

A. Confidential communications.

1. State entities must accommodate any reasonable request by a patient to receive confidential communications from a state entity regarding health information by alternative means or at alternative locations provided that all the following conditions are satisfied:
   a. The request is provided in writing
   b. An alternative address or other method of contact is provided
   c. When appropriate, information as to how payment, if any, will be handled

   [45 C.F.R. § 164.522(b)(2)]
2. State entities and business associates must communicate the request for confidential communication within two (2) days of the request to each other.
3. A patient is not required to provide an explanation for the request and the request cannot be denied solely because an explanation was not given. State entities may not ask for an explanation from the patient as to why the request is being made.
   [45 C.F.R. § 164.522(b)(2)(iii)]
4. State entities are responsible to develop a process to ensure the appropriate patient address and/or phone number is recorded in the system or medical record and is used when communicating with the patient.

B. Documentation. State entities are responsible to do all the following:

1. Document all requests for confidential communication
2. Document the reason for a denial of request for confidential communication, if applicable
3. Maintain correspondence and associated documentation related to patient requests for confidential communications, including denials, in the patient's medical record, in accordance with the records retention policy (*for a minimum of six (6) years)*

[45 C.F.R. § 164.530(j)]

IV. References

45 C.F.R.

- § 164.522(b)
- § 164.530(j)

V. Related Policies

SHIPM Chapter 1 – CalOHII Authority
SHIPM Chapter 4 – Business Associate Agreement

VI. Attachments

None

SHIPM Definitions

SHIPM Definitions		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

Term	Definition
Access	*IT related*: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. [source: 45 C.F.R. § 164.304] *Non-IT related*: The right of an individual, or his or her patient representative, to inspect and/or obtain a copy of the individual's health information. [source: 45 C.F.R. § 164.524]
Acquired Immunodeficiency Syndrome (AIDS)	A disease of the immune system characterized by increased susceptibility to opportunistic infections, to certain cancers and to neurological disorders. [source: Dictionary.com website]
Addressable *[security]*	There are two classes of security safeguards - *required* and *addressable*. Addressable safeguards allow an organization to determine what is reasonable and appropriate, considering the likely contribution to protecting health information for that specific organization. The organization must either implement the requirement, or document why the requirement would not be appropriate and implement an equivalent alternative safeguard measure. [source: 45 C.F.R. § 164.306(d)(3) *(paraphrased)*]
Administrative Safeguards *[security]*	Administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information, and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that health information. [source: 45 C.F.R. § 164.304]
Agents	A person or business authorized to act on another's behalf. [source: Dictionary.com website]
Audit Logs	A chronological record of information system activities, including records of system accesses and operations performed in a given period. [source: NIST SP 800-53 Rev. 5]

Term	Definition
Audit Trails	A chronological set of logs and records used to provide evidence of a system's performance or personnel activity that took place on the system, and used to detect and identify intruders. [source: CA Department of Technology website - Technical Definitions]
Authentication	*IT related*: verifying the identity of a user, process, or device, as a prerequisite to allowing access to resources in an information system. [source: CA Department of Technology website - Technical Definitions] *Non-IT related*: the corroboration that a person is the one claimed. [source: 45 C.F.R. § 164.304]
Authorization	*IT related*: the act of granting a user, program, process or device access to information assets after proper identification and authentication are obtained. [source: CA Department of Technology website - Technical Definitions] *Non-IT related*: a detailed document that gives covered entities permission to use health information for specified purposes which are generally other than treatment, payment, or healthcare operations, or to disclosed health information to a third party specified by the individual. Relates to past, present, or future physical or mental conditions. [source: 42 C.F.R. § 2.31, § 2.33; 45 C.F.R. § 164.508; CA Civil Code § 56.11; CA Health and Safety Code § 11845.5(b); CA Welfare and Institution Code § 5328.7]
Availability	*IT related*: the reliability and accessibility of information assets to authorized personnel in a timely manner. [source: CA Department of Technology website - Technical Definitions] *Non-IT related*: the property that data or information is accessible and usable upon demand by an authorized person. [source: 45 C.F.R. § 164.304]

Term	Definition
Breach	The unauthorized acquisition, access, use or disclosure of health information in a manner not permitted, which compromises the security or privacy of the health information. This includes both: • Unencrypted data that was, or is reasonably believed to have been, acquired by an unauthorized person, and • Encrypted data that was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or has been reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that data readable or usable [source: 45 C.F.R. § 164.402; CA Civil Code § 1798.29]
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of health information on behalf of, or provides services to, a covered entity. BAs may include, but not limited to: • Organizations that provide services (e.g., claims processing, clearing houses, data analysis, utilization review, quality assurance, billing, legal) on behalf of a covered entity where access to health information is required • A person or organization "that offers a personal health record to one or more individuals on behalf of a covered entity…" • A "subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate…" A member of the covered entity's workforce is not a Business Associate. [source: 45 C.F.R. § 160.103 *(paraphrased)*]
Business Associate Agreement (BAA)	A contract between a HIPAA covered entity and a HIPAA business associate (BA). The contract protects health information in accordance with HIPAA guidelines. [source: 45 C.F.R. § 164.504(e) *(paraphrased)*]
CA	A two-letter abbreviation used to represent California. [source: USPS website]
Confidentiality	A security and privacy principle that works to ensure that information is not disclosed to unauthorized persons. [source: CA Department of Technology website - Technical Definitions; 45 C.F.R. § 164.304]

Term	Definition
Covered Entity	The following individuals or organizations that directly handle health information: • A health plan • A health care clearinghouse • A health care provider who transmits any health information in electronic form in connection with a standard transaction covered by HIPAA [source: 45 C.F.R. § 160.103]
Covered Functions	Functions performed by a covered entity that make the entity a health care provider, health plan, or health care clearinghouse under the HIPAA Administrative Simplification Rules. [source: HHS National Institutes of Health website *(paraphrased)*]
De-identified Information	Information redacted to remove any identifying information and prevent the information from being used to re-identify the patient. *The California Health and Human Services' Data Playbook site provides a Data De-Identification Guidelines resource.* *This process of de-identification mitigates privacy risks to patients and thereby supports the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research and other endeavors.* [source: 45 C.F.R. § 164.514(a); HHS website *(paraphrased)*]
Designated Record Set	A group of records maintained by, or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a Health Plan; or information used in whole or in part to make care-related decisions. [source: 45 C.F.R. § 164.501]
Developmental Services Records	All information and records obtained in the course of providing intake, assessment, and services covered under Division 4.1, Division 4.5, Division 6, or Division 7 of the Welfare and Institutions Code to persons with developmental disabilities. [source: CA Welfare and Institutions Code § 4514]

Term	Definition
Direct Treatment Relationship	A treatment relationship between a patient and a health care provider that is not an indirect treatment relationship. [source: 45 C.F.R. § 164.501] *Indirect Treatment Relationship: A relationship between a patient and a health care provider, where the provider:* • *Delivers health care to the patient based on the orders of another health care provider* • *Typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides services or products or reports to the patient*
Disability Rights California	The disability rights protection and advocacy agency for the State of California, authorized by federal and state regulations. The agency is further described on its website at Disability Rights California. [source: 42 U.S.C. § 15043(a), and § 10805; CA Welfare and Institutions Code §§ 4900 - 4903]
Disclose	The disclosure, release, transfer, dissemination, or to otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity. [source: 45 C.F.R. § 160.103; CA Civil Code § 1798.3] *To communicate any information identifying a patient as being or having been diagnosed with a substance use disorder, having or having had a substance use disorder, or being or having been referred for treatment of a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person.* [source: 42 C.F.R. § 2.11]
Electronic Data Interchange (EDI)	The electronic exchange, via information systems, of business data in standard electronic formats between business partners. [source: EDI website (paraphrased)]
Electronic Health Record	A real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision making. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting. [source: Health IT.gov website *(paraphrased)*]

Term	Definition
Employer	Any person or organization acting directly to engage the services of members of a workforce, or indirectly in the interest of a person or group engaging the services of members of a workforce, in relation to an employee benefit plan; and includes a group or association of employers acting for an employer in such capacity. [source: ERISA - 29 U.S.C. § 1002(5); see also 45 C.F.R. § 160.103]
Encryption	Rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security. [source: CA Civil Code § 1798.29; see also 45 C.F.R. § 164.304]
Federal Trade Commission Act (FTC Act)	The FTC Act prohibits organizations "from engaging in deceptive or unfair acts or practices in or affecting commerce." With regard to an authorization, it must meet HIPAA requirements as well as ensure it does not create a deceptive or misleading impression. Consult the FTC website for more information on FTC Act and authorizations. [source: Federal Trade Commission website]
Fundraising	The process of gathering voluntary contributions of money or other resources, by requesting donations from individuals, businesses, charitable foundations, or governmental agencies. [source: Wikipedia website (*paraphrased*)]
Genetic Information	Information about any of the following: • A patient's genetic tests; • The patient's family members' genetic tests; • The manifestation of a disease or disorder in family members of such a patient; *or* • Any request for or receipt of genetic services or participation in clinical research which includes genetic services by the patient or any family member of the patient. Genetic information includes: • Information about the fetus of a patient or family member who is pregnant; *and* • Any embryo legally held by a patient or family member utilizing an assisted reproductive technology. *Genetic services as used in the definition of "genetic information" means: a genetic test, genetic counseling, or education*. [source: 42 U.S.C. § 2000ff(4) *(paraphrased)*]

Term	Definition
Group Health Plan	A program that, directly or through insurance or reimbursement, provides services and goods paid for as medical care to employees or their dependents, ***and***: • Has 50 or more participants, *or* • Is administered by an entity other than the employer that established and maintains the plan Examples include: • Employer-provided health insurance or HMO participation • Union-sponsored health plans • Multi-jurisdictional public employee health plans • Employer-coalition reimbursement plans • A health insurance issuer or HMO providing health care good and services to the group health plan [source: 45 C.F.R. § 160.103; 29 U.S.C. § 1002(1); 42 U.S.C. §§ 300gg-91(a)(1)]
Health Care Clearinghouse	A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: • Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a HIPAA compliant transaction • Receives a HIPAA compliant transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity [source: 45 C.F.R. § 164.103]
Health Care Component	The part(s) (or component(s)) of a hybrid entity that perform functions covered by HIPAA. [source: 45 C.F.R. § 164.103, and § 164.105(a) *(paraphrased)*]

Term	Definition
Health Care Operations	Activities relating to covered functions of a business associate, health care clearinghouse, health care plan, health care provider or hybrid entity. Including, but not limited to: • Conducting quality assessment and improvement activities; patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment • Licensing and accreditation • Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities • Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care • Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs • Business planning and development • Business management and general administrative activities of the entity [source: 45 C.F.R. § 164.501; CA Civil Code § 56.10(c)]

Term	Definition
Health Care Plan or Health Plan	An individual or group plan that provides, or pays the costs of, medical care and includes the following, singly or in: • A group plan, a health insurance issuer, a health care service plan • An HMO • Part A, B, or D of the Medicare program, or a supplemental policy • Medicaid program under title XIX • A long-term care policy excluding a nursing home fixed indemnity policy • An employee welfare benefit plan • A health care program for uniformed services • A veterans health care program • An Indian Health Services program • The Federal Employees Health Benefits Program • An approved state child health plan • A Medicare Advantage program • A high risk pool established under state law to provide health insurance coverage or comparable coverage • Any other individual or group plan or combination of individual or group plans that provides or pays for the cost of medical care [source: 45 C.F.R. § 160.103; 42 U.S.C. 300gg-91(a)(2); CA Civil Code § 56.05]
Health Care Provider	Any person or organization that furnishes, bills, or is paid for health care in the normal course of business. Examples include: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies Health Care Providers must comply with HIPAA, only if they transmit health information electronically in connection with a HIPAA covered transaction. [source: 45 C.F.R. § 160.102, and § 160.103]

Term	Definition
Health Care Services	Care, services or supplies related to the health of a patient. It includes, but is not limited to: • Preventative, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, of functional status, of an individual or that affects the structure or function of the body; and • Sale of dispensing of a drug, device, equipment, or other item in accordance with a prescription. [source: 45 C.F.R. § 160.103]
Health Information	Any name in combination with any other information related to the provision of health care that can lead a person to reasonably identify the patient. *This SHIPM definition incorporates and synthesizes State of CA and federal definitions, including:* • *Protected Health Information* • *Electronic Health Information* • *Individually Identifiable Health Information* • *Personal Information* • *Medical Information* • *Confidential and Private Information* *Special note: Health Information as used in the SHIPM does not include information and records covered by other federal or state laws regarding substance use disorder treatment records, mental/behavioral health records, developmental services records, HIV, genetic information.* *See policies covering Specially Protected Health Information for these rules.* [source: 45 C.F.R. § 160.103; CA Civil Code § 56.05, and § 1798.3]
Health Information Exchange (HIE)	The capability to electronically move health information among disparate health care information systems, and maintain the meaning of the information being exchanged. *The goal of HIE is to facilitate access to, and retrieval of, clinical data to provide safe, timely, efficient, effective, equitable and patient-centered care.* [source: Health Information and Management Systems Society (HIMSS) website]

Term	Definition
Health Information Organization (HIO)	An organization that oversees and governs the exchange of health information among stakeholders within a defined geographic area, for improving health and care in that community. [source: HIMSS – FAQ: Health Information Exchange website]
Health Oversight Activities	The oversight of the health care system (whether public or private), as well as government benefit programs, entities subject to government regulatory programs and entities subject to civil rights laws. These oversight activities include: • Audits • Civil, administrative or criminal investigations • Inspections • Licensure or disciplinary action • Civil, administrative or criminal proceedings or actions [source: 45 C.F.R. § 164.512(d)(1) *(paraphrased)]*
Health Oversight Agency	A person, or entity, at any level of the federal, state, local, or tribal government that oversees the health care system or requires health information to determine eligibility, or compliance, or to enforce civil rights laws. Examples include: • State and county licensing agencies • Department of Justice and their civil rights enforcement activities • State Medicaid fraud control units • Food and Drug Administration [source: 45 C.F.R. § 164.501 (*paraphrased*)]
HIV/AIDS Test Results	The results of any clinical test, laboratory or otherwise, used to identify HIV and/or AIDS, a component of HIV and/or AIDS, or antibodies or antigens to HIV. [source: CA Health and Safety Code § 120775(c)]
Human Immunodeficiency Virus (HIV)	A variable retrovirus that invades and inactivates helper T cells of the immune system and is a cause of AIDS and AIDS-related complex. [source: Dictionary.com website]

Term	Definition
Hybrid Entity	A single legal entity that is: • A business associate, health care clearinghouse, health care plan, or health care provider whose business activities include both HIPAA covered and non-covered functions; and • That designates the HIPAA covered health care components and creates adequate "firewalls" between covered and non-covered health care components in accordance with the law. Example of a hybrid entity: A state entity that provides health care and health care oversight functions [source: 45 C.F.R. § 164.103 *(paraphrased)*]
Implementation	The act of fulfillment, or carry out. To put into effect according to or by means of a definite plan or procedure. *Implementation also includes initializing and complying with policies and procedures, as well as maintaining them.* [source: Dictionary.com] For policies and procedures (P&Ps) – Implementation includes training all workforce members on the specifics of the policies and procedures, complying with all requirements in the SHIPM, and maintaining P&Ps by reviewing and revising as business practices and/or regulations change. [source: SHIPM Chapter 1, CalOHII Authority]
Incidental Disclosure	A secondary disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted. For example, a health care professional calling out a patient's name in a crowded waiting room. [source: HHS website]
Individually Identifiable Health Information	Information that is a subset of health information, including demographic information, collected from a patient, *and*: • Is created or received by a health care provider, health plan, employer or health care clearinghouse, and • Relates to past, present, or future physical or mental health or condition of a patient; or the past, present, or future payment for the provision of health care to a patient, *and* ○ That identifies the patient, *or* ○ With respect to which there is a reasonable basis to believe the information can be used to identify the patient [source: 45 C.F.R. § 160.103]

Term	Definition
Institutional Review Board (IRB) / Privacy Board	An administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated. IRBs have the authority to approve, require modifications in, or disapprove all research activities that fall within its jurisdiction. [source: HHS website; 45 C.F.R. §§ 164.512(i)(1)(i)(A) - (B)]
Integrity	The property that data or information has not been altered or destroyed in an unauthorized manner. [source: 45 C.F.R. § 164.304]
Law Enforcement Official	An officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision or a state or territory, or an Indian tribe, who has arrest powers. Examples include: • Peace officers • District attorneys • Sheriffs [source: 45 C.F.R. § 164.103; CA Penal Code § 830, and § 834]
Limited Data Set	Health information that excludes the following direct identifiers of the patient, or of relatives, employers, or household members of the patient: • Names • Postal address information, other than town or city, state, and zip code • Telephone and Fax numbers • Electronic Mail addresses • Social Security numbers • Medical record numbers • Health Plan beneficiary numbers • Account numbers • Certificate / License numbers • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Universal Resource Locators (URLs) • Internet Protocol (IP) address numbers • Biometric identifiers, including finger and voice prints • Full face photographic images and any comparable images [source: 45 C.F.R. § 164.514(e)(2)]

Term	Definition
Marketing	A communication about a product or service that encourages recipients of the communication to purchase or use the product or service. The entity may receive financial remuneration in exchange for making the communication. [source: 45 C.F.R. § 164.501 *(paraphrased)*]
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integrations (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. [source: NIST SP 800-53 Rev. 5]
Mental Health Records	Information and records related to all involuntary treatment; all voluntary treatment at a state or local hospital, developmental center, psychiatric hospital or unit, obtained in the course of providing services under the following provisions of California's Welfare and Institutions Code: • Division 4 and 5 (concerning mental health services) • Division 6 (concerning voluntary admissions to state hospitals) • Division 7 (concerning psychiatric services in county hospitals) Patient records, or discrete portions thereof, specifically related to evaluation or treatment of a mental disorder. Mental health records include, but are not limited to, all alcohol and substance use records. [source: CA Civil Code § 56.30; CA Welfare and Institutions Code § 5328]
Minimum Necessary	The amount of information, to the extent necessary, to accomplish the intended purpose of a use, disclosure or request. [source: 45 C.F.R. § 164.502(b), and § 164.514(d)]
Mobile (Computing) Devices	Portable computing devices that can connect by cable, telephone wire, wireless transmission, or via any internet connection to an IT infrastructure and/or data systems. Examples include: • Laptops • Cellular smart phones • Personal digital assistants • Blackberries • Tablet personal computers • Portable hard drives [source: CA Department of Technology website - Technical Definitions]

Term	Definition
Multiple Covered Functions	Those functions of a covered entity that operationally designate the entity as any combination of the following under the HIPAA Administrative Simplification Rules: health care provider, health plan, or health care clearinghouse. [source: National Governors Association website (*paraphrased*)]
Patient	Any natural person who is receiving health care services from a health care provider and to whom the health information pertains. *This SHIPM definition combines terms from:* • *HIPAA – Person and Individual* • *CMIA (CA Civil Code § 56.10) – Enrollee and Patient* • *IPA (CA Civil Code § 1798) – Individual and Person* [source: 42 C.F.R. § 2.11; 45 C.F.R. § 160.103; CA Civil Code § 56.05, and § 1798.3]
Patient's Representative	A person who: • Has the authority under law to make health care decisions for another person, or • Has the authority to administer the estate of a deceased person (including executor) *An individual should not be treated as the patient's representative, if:* • *There is a reasonable belief that the individual has or will abuse/neglect/treat the patient with violence, or* • *May endanger the patient if the information is provided to the individual, and* • *It would not be in the best interest of the patient to treat the individual as the patient's representative* [source: HHS website; 45 C.F.R. § 164.502(g)]
Payment	The activities undertaken by: • A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan (except as prohibited under § 164.502(a)(5)(i)); or • A health care provider or health plan to obtain or provide reimbursement for the provision of health care (including billing, claims management, determination of eligibility for health benefits, justification of charges, utilization review). [source: 45 C.F.R. § 164.501; CA Civil Code § 56.10(c)]
Pharmaceutical Company	Any company or business (including its agents or representatives) that manufactures, sells, or distributes pharmaceuticals, medications, or prescription drugs. [source: 45 C.F.R. § 160.103]

Term	Definition
Physical Safeguards *[security]*	The physical measures and policies and procedures used to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusions. [source: 45 C.F.R. § 164.306 (paraphrased)]
Plan Sponsor	The person or organization that arranges to provide health care goods and services for a group of participants by establishing or maintaining a group health plan (GHP). Examples include: • An employer in the case of a GHP established or maintained by a single employer for the benefit of employees or their dependents; • An employee organization (including unions or guilds) in the case of a group health plan established or maintained by an employee organization; • An association, joint board of trustees, or similar group of representatives of the parties in the case of a GHP established and maintained by two or more parties (including multiple employers, or an employer and an employee organization). [source: 29 U.S.C. § 1002(16)(B)]
Policy	Defines an organization's values and expected behaviors (the WHAT and WHY) – establish measurable objectives and expectations for the workforce, assign responsibility for decision making, and define enforcement and consequences for violations. [source: Centers for Medicare and Medicaid Services (CMS) (2007) Organizational, Policies and Procedures and Documentation Requirements – Security Rule Educational Paper Series]
Privacy	The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves. [source: CA Department of Technology website - Technical Definitions]
Procedure	Describes how the organization will carry out the approach, setting forth explicit step-by-step instructions on how to implement the organization's policy (the HOW, WHERE and WHEN). [source: CMS (2007) Organizational, Policies and Procedures and Documentation Requirements – Security Rule Educational Paper Series]

Term	Definition
Professional Judgment	The analysis and conclusions of a licensed medical, mental health, or developmental disabilities service provider regarding the use and disclosure of health information and its impact on the patient. Examples of professional judgment include: • Whether the patient's representative should have access to the health information • Whether another person who is in the facility, or might come to the facility, could reasonably cause harm or danger to the patient • Whether disclosing the patient's location within the facility implicitly would give information about the patient's condition • Whether it is necessary or appropriate to give information about patient status to family and friends [source: 45 C.F.R. § 164.502, § 164.510, § 164.514, and § 164.524]
Program	Synonymous with "Substance Use Disorder Treatment Program" • An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or • An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment or referral for treatment; or • Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who is identified as such providers. [source: 42 C.F.R. § 2.11]
Prominent	Standing out so as to be easily seen, conspicuous, particularly noticeable. [source: Dictionary.Com website] Best practice from 2018 HIPAA Summit – OCR clarification session: "Do not put it [NPP] in the footer of page/site (e.g., place NPP button/link on website landing page)."

Term	Definition
Psychotherapy Notes	Notes recorded (in any medium) by a qualified professional documenting or analyzing the contents of conversation during a private or group, joint or family counseling session and that are separated from the rest of the individual's medical record. *Note: Medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and summary information (diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date) are NOT considered psychotherapy notes.* [source: 45 C.F.R. § 164.501]
Public Health Authority	An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. [source: 45 C.F.R. § 164.512(b) and Public Health Authority Disclosure Request Checklist]
Qualified Professional	A person who has education, training, licensure, certification, or experience to oversee, or to make the particular decision at issues as required by federal or state law. [source: CalOHII]

Qualified Service Organization	An individual or entity who:
	• Provides services to a part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and
	• Has entered into a written agreement with a part 2 program under which the individual or entity:
	  ○ Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the part 2 program, it is fully bound by the regulations in this part; and
	  ○ If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by the regulations in this part.
	
	[source: 42 C.F.R. § 2.11]

Term	Definition
Research	A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge. [source: 45 C.F.R. § 164.501]
Security	The administrative, physical and technical safeguards in, or protecting, an information system. [source: 45 C.F.R. § 164.304]
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies. [source: CA Department of Technology website - Technical Definitions; 45 C.F.R. § 164.304]
Specially Protected Health Information	Any information regarding a patient's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional that requires special protections under the law, including substance use disorder treatment records, mental health records, psychotherapy notes, behavioral health records, HIV, AIDS, and genetic information. [source: AHIMA Glossary of Terms *(paraphrased)*]
State Entity	State departments, boards, commissions, programs, and other organizational units of the executive branch of state government. [source: CA Health and Safety Code § 130302]
Substance Use Disorder	A cluster of cognitive behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. This does not include caffeine or tobacco. [source: 42 C.F.R. § 2.11]

Term	Definition
Substance Use Disorder Treatment Program	Synonymous with "Program": • An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or • An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment or referral for treatment; or • Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who is identified as such providers. [source: 42 C.F.R. § 2.11]
Substance Use Disorder Treatment Records	Any information: • Whether recorded or not, created by, received, or acquired by a part 2 program relating to a patient. Records include both paper and electronic records; • That identifies a patient as an individual with a substance use disorder either directly, by reference to other publicly available information, or through verification of such an identification by another person; • Is drug abuse information obtained by a federally assisted drug abuse program after March 20, 1972; or is alcohol abuse information obtained by a federally assisted alcohol abuse program after May 13, 1974 (or is obtained prior to this date and maintained by such a treatment program after this date as part of an ongoing treatment episode which extends past this date); and • Is for the purpose of treating substance use disorder, making a diagnosis for this treatment, or making a referral for this treatment. This includes patient substance use disorder treatment records as referenced in applicable state law. [source: 42 C.F.R. § 2.11 and § 2.12(a)(1); CA Civil Code § 56.30(i)]
Technical Safeguards	The technology and policy and procedures in use that protect and control access to electronic health information. [source: 45 C.F.R. § 164.304]

Term	Definition
Telehealth	The mode of delivering health care services and public health via telecommunications system(s) and technologies to facilitate the diagnosis, consultation, treatment, education, care management, and self-management of a patient's health care while the patient is at one location and the health care provider is at another site without the physical presence of the patient. *Telehealth includes:* • *Real-time interactions between a patient and a health care provider* • *Transmission of patient health information to the health care provider, or* • *Medical advice provided by means of telephonic communications between a patient and a health care provider in which the health care professional's primacy function is to provide the patient a telephonic assessment, evaluation or advice to the patient's questions regarding his or her medical care or treatment, or that of a family member.* [source: CA Business and Professions Code § 2290.5(a); CA Health and Safety Code § 1348.8(c)]
Transactions and Code Sets (TCS)	The collective name given to federal regulations standardizing and administratively simplifying the process, procedures and data elements used to electronically capture, store, and move health information. *Transactions* are electronic exchanges involving the movement of information between parties for health care purposes. *Code sets* are groups of codes used to categorize diagnoses, procedures, medical equipment and medications, and used in all transactions. • *HCPCS (Ancillary Services/Procedures)* • *CPT-4 (Physicians Procedures)* • *CDT (Dental Terminology)* • *ICD-9 (Diagnosis and hospital inpatient Procedures)* • *ICD-10 (As of October 1, 2015)* • *NDC (National Drug Codes)* • *National Identifiers: Patient, Provider, Payer/Health Plan, Employer* [source: HHS website]

Term	Definition
Treating Provider Relationship	Regardless of whether there has been an actual in-person encounter: • A patient is, agrees to, or is legally required to be diagnosed, evaluated and/or treated, or agrees to accept consultation, for any condition by an individual or entity, and; • The individual or entity undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient, or consultation with the patient, for any condition. [source: 42 CFR § 2.11]
Treatment	The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. [source: 45 C.F.R. § 164.501]

Treatment Relationship	One of two methods by which a health care provider delivers health care services to a patient:
	• *Indirect* is a relationship between an individual and a health care provider in which:
	  ○ The health care provider delivers health care services or products to the patient based on the orders of another health care provider, and
	  ○ The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the patient.
	• *Direct* is a relationship between a health care provider and a patient that is not an indirect treatment relationship (i.e., the provider delivers health care services or products to a patient based on professional judgment and personal observation).
	If Part 2 treatment, see Treating Provider Relationship.
	[source: 45 C.F.R. § 164.501]

Term	Definition
Underwriting	Activities related to the measurement of risk exposure and the creation, renewal or replacement of a contract for health insurance benefits. Examples include: • Determinations of eligibility • Determinations of the cost of premiums • Determinations of the applicability of exclusion for a preexisting condition [source: 42 U.S.C. § 1320(d)(9)]
Whistleblower	A workforce member who alleges wrong-doing or conduct by his/her organization of the sort that violates the law, regulation, executive order, rule of court, unsafe working conditions, SAM, state contracting manual, or gross mismanagement; and is reported to an authority (internally or externally) to investigate, discover or correct the problem. [source: 5 U.S.C. § 2302(b)(8) (*paraphrased*); CA Labor Law § 1102.5]
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. [source: 45 C.F.R. § 160.103]
Workstation	An electronic device that performs computing functions and stores electronic media in its immediate environment (e.g., desktop computer, laptop computer, mobile devices or any other computing device). [source: 45 C.F.R. § 164.304]

Summary of Privacy Laws

Summary of Privacy Laws		
Review Date: 06/01/2021	Revision Date: 06/01/2021	Attachments: No

Due to the complex nature of privacy laws, SHIPM users should review and consult the materials in this section with their legal counsel.

Federal

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA describes privacy, security, patient rights, and health care transactions requirements for health care entities. It sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	45 C.F.R. Parts 160 and 164
Who is Covered?	Covered Entities: 1) health plans; 2) healthcare clearinghouses; and 3) health providers that conduct certain healthcare transactions electronically. Business Associates of a HIPAA covered entity.
What information is covered?	Protected Health Information (PHI)*: all "individually identifiable health information" held or transmitted by a HIPAA covered entity or its business associate, in any form or media, whether electronic, paper, or oral. *Exempts educational records covered by Family Educational Rights and Privacy Act (FERPA).
Patient breach notification requirement?	YES
Patient access requirement?	YES
Patient amend/correct requirement?	YES
Limitations on disclosure?	YES
Respond to a subpoena?	YES
Private right of action?	NO
Liability for violation	Fines levied by federal oversight (U.S. Health and Human Services, Office of Civil Rights)

Substance Use Disorder (SUD)

42 C.F.R. Part 2 sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	42 C.F.R. Part 2
Who is Covered?	Federally assisted SUD treatment programs that meet the definition of a Program.
What information is covered?	Information that would identify a patient as having a SUD and allow very limited disclosures of information without patient authorization.
Patient breach notification requirement?	NO
Patient access requirement?	YES
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	NO
Private right of action?	YES
Liability for violation	• Entity Liability • Criminal Liability

Family Educational Rights and Privacy Act (FERPA)

FERPA describes privacy and student/family rights requirements for educational entities. It sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	20 U.S.C. § 1232g; 34 C.F.R. Part 99
Who is Covered?	All schools that receive funds under an applicable program of the U.S. Department of Education.
What information is covered?	Education records
Patient breach notification requirement?	NO
Patient access requirement?	YES
Patient amend/correct requirement?	YES
Limitations on disclosure?	YES
Respond to a subpoena?	YES
Private right of action?	NO
Liability for violation	Loss of federal funding by U.S. Department of Education

The Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)

WIC sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	7 C.F.R. §§ 246.3, 246.26
Who is Covered?	WIC Program, its contractors—including WIC local agencies—as well as subcontractors
What information is covered?	Any information about a WIC applicant or participant, whether it is obtained from the applicant or participant, another source, or generated as a result of WIC application, certification, or participation, that individually identifies an applicant or participant and/or family member(s). Applicant or participant information is confidential, regardless of the original source and exclusive of previously applicable confidentiality provided in accordance with other federal, state, or local law.
Applicant/participant breach notification requirement?	NO * *Consult the WIC contract for specific contractual requirements for breach notification.
Applicant/participant access requirement?	YES
Applicant/participant amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	Limited; WIC is required to quash a subpoena for a WIC applicant/participant's confidential information unless disclosing is in the best interest of the WIC Program. (7 C.F.R. § 246.26(i).)

The Supplemental Nutrition Assistance Program (SNAP)

SNAP sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	7 C.F.R. § 272.1
Who is Covered?	State and local welfare agencies providing SNAP (known in California as CalFresh)
What information is covered?	All information obtained from SNAP applicant or recipient households.
Patient breach notification requirement?	NO
Patient access requirement?	YES
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES

State of California

Information Practices Act (IPA)

The IPA sets limitations on collection and retention of data. It describes individual rights requirements and sets restrictions on access, use, and disclosure.

Item	***Information***
Citation(s)	Cal. Civ. Code § 1798 et seq.
Who is Covered?	State agencies, departments, offices, officers, etc.
What information is covered?	Personal Information: any information maintained by an agency that identifies or describes an individual.
Patient breach notification requirement?	YES
Patient access requirement?	YES
Patient amend/correct requirement?	YES
Limitations on disclosure?	YES
Respond to a subpoena?	YES
Private right of action?	YES
Liability for violation	• Entity liability • Personal liability (potential job loss)

Confidentiality of Medical Information Act (CMIA)

The CMIA sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	Cal. Civ. Code § 56 et seq.
Who is Covered?	Health providers, health plans, and their contractors.
What information is covered?	Medical information[3]
Patient breach notification requirement?	*Refer to* Health Facilities and Data Breach
Patient access requirement?	YES
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	YES
Private right of action?	YES
Liability for violation	Entity liability

[3] Note, while CMIA covers privacy of most health information, it does not cover all. Health information covered by Cal. Welf. & Inst. Code §§ 4514, 5328, and 10850 et seq., 42 C.F.R. Part 2, and Cal. Health & Safety Code § 11845.5 are not covered by CMIA.

California Consumer Privacy Act (CCPA)

The CCPA sets restrictions on access, use, and disclosure. It describes individual rights.

Item	*Information*
Citation(s)	Cal. Civ. Code § 1798.100 et seq.
Who is Covered?	For-profit businesses* that collect consumers' personal information and meet certain threshold requirements for annual revenue or number of consumers of whom they receive, buy, sell, or share personal information. *Exempts health providers covered by HIPAA or the CMIA.
What information is covered?	Personal Information*: information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. *Exempts data covered by HIPAA or the CMIA.
Patient breach notification requirement?	NO
Patient access requirement?	YES
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	YES
Private right of action?	YES
Liability for violation	• Entity liability • Injunctive or declaratory relief

Patient Access to Health Records Act (PAHRA)

The PAHRA describes a patient's right of access or denial of access to health information.

Item	*Information*
Citation(s)	Cal. Health & Safety Code §§ 123100 – 123149.5
Who is Covered?	Health providers
What information is covered?	Medical records
Patient breach notification requirement?	NO
Patient access requirement?	YES
Patient amend/correct requirement?	NO; however, a patient has the right to add a written addendum to the record
Limitations on disclosure?	NO
Private right of action?	YES
Liability for violation	Entity liability

Lanterman-Petris-Short Act (LPS) – Mental Health

LPS describes privacy requirements and it sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	Cal. Welf. & Inst. Code § 5328 et seq.
Who is Covered?	Generally, county or city mental health departments, state hospitals, or other public or private entities (such as community mental health clinics).
What information is covered?	Information and records obtained in the course of providing services to involuntarily, and some voluntary, recipients of services are confidential and specially protected under LPS.
Patient breach notification requirement?	NO
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	NO
Private right of action?	YES
Liability for violation	• Entity liability • Personal liability

Lanterman Developmental Disabilities Services Act (LDDA) – Developmental Disabilities

LDDA sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	Cal. Welf. & Inst. Code § 4514
Who is Covered?	California Department of Developmental Services (DDS) and regional centers under contract with the DDS.
What information is covered?	All information and records obtained in the course of providing intake, assessment, and services for persons with developmental disabilities.
Patient breach notification requirement?	NO
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	NO
Private right of action?	YES
Liability for violation	• Entity liability • Personal liability

California Substance Use Disorder Records - SUD

California SUD law sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	Cal. Health & Safety Code § 11845.5
Who is Covered?	Entities that are licensed by the California Department of Health Care Services (DHCS) in connection with SUD diagnosis and treatment.
What information is covered?	Information that would identify a patient as having a SUD and allow very limited disclosures of information without patient authorization.
Patient breach notification requirement?	NO
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	NO
Private right of action?	NO

Health Facilities and Data Breach

Breach reporting requirement to licensing entity.

Item	*Information*
Citation(s)	Cal. Health & Safety Code § 1280.15
Who is Covered?	A clinic, health facility, home health agency, or hospice licensed pursuant to Cal. Health & Safety Code §§ 1204, 1250, 1725, or 1745.
What information is covered?	Medical information
Patient breach notification requirement?	YES
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	NO
Private right of action?	NO
Liability for violation	Fines leveed by state oversight (California Department of Public Health)

Data Breach of Customer Records

Breach reporting requirements for persons and businesses.

Item	*Information*
Citation(s)	Cal. Civ. Code § 1798.82
Who is Covered?	Persons and businesses conducting business in California
What information is covered?	Personal information as defined in subdivision (h) of Cal. Civ. Code § 1798.82.
Patient breach notification requirement?	YES
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	NO
Private right of action?	NO
Liability for violation	Entity liability

Public Social Services

This law sets restrictions on access, use, and disclosure.

Item	*Information*
Citation(s)	Cal. Welf. & Inst. Code § 10850
Who is Covered?	California Department of Social Services and county welfare departments
What information is covered?	All applications and records concerning any individual made or kept by any public officer or agency in connection with any form of public social services for which grants-in-aid are received from the United States government.
Patient breach notification requirement?	NO
Patient access requirement?	NO
Patient amend/correct requirement?	NO
Limitations on disclosure?	YES
Respond to a subpoena?	NO