

**Compliance Review Worksheet Tool Instructions**

Please complete requested information on "Organization Info" tab (in the non-shaded areas)

Please complete requested information on "Privacy", "Security", "Administrative" and "Patient Rights" tabs (in the non-shaded areas)

If you/your organization respond with "Partially" or "No" to any questions, additional explanation or comment is required in the "Assessment Organization's Comments / Explanations" column

You may include additional information and comment in the "Assessment Organization's Comments / Explanations" column, if you would like to explain any "Yes" or "Not Applicable" answers

Please provide 1 (one) worksheet for your organization's response to the Compliance Review Assessment (if your organization splits the completion of the worksheet to a number of resources in your organization, the Compliance Review Assessment coordinator for your organization is responsible to ensure only one response is submitted to CalOHII on behalf of your organization)

Once your organization's Compliance Review Assessment worksheet is complete, please upload to your specified CalOHII SharePoint site

Once the worksheet has been submitted, the worksheet is protected and revisions aren't permitted (if you have revisions, you may submit a new worksheet to CalOHII - if it is submitted within the time allowed to complete the Compliance Tool)

Please indicate those items that are Confidential and not subject to Public Records Act requests in the "Assessment Organization's Comments / Explanation" column. CalOHII does not make that determination on your Organization's behalf.

**Who to Contact if You Experience Difficulties or Have Questions**

**Worksheet technical difficulties:** If you experience technical difficulties with the worksheet, please contact Wanda Yepez at (916) 651-3366; or Betsy Figueiro-Steinbrueck at (916) 651-2060

**How to fill out worksheet:** If you have questions regarding how to fill out the worksheet, or need clarification regarding the questions, please contact Wanda Yepez at (916) 651-3366; or Betsy Figueiro-Steinbrueck at (916) 651-2060

**SharePoint technical difficulties or questions:** If you have questions or experience technical difficulties with the SharePoint site established for the collection of your responses, artifacts, and documentation, please contact Wanda Yepez at (916) 651-3366; or Bob Summers at (916) 651-6907

**General Questions:** If you have general questions regarding the Compliance Assessment and related activities, please contact Wanda Yepez at (916) 651-3366; or Betsy Figueiro-Steinbrueck at (916) 651-2060

**Special Information Concerning the Compliance Review Assessment Tool**

Any SHIPM Topic that includes an "(A)" designation following a topic description means an artifact was requested as part of the overall assessment

**EXAMPLE**

Compliance Program Sequence #	SHIPM Policy #	SHIPM Topic	Requirement	Question	Organization's Response / Answer <i>(Please provide explanation why you've answered "Yes", "Partially", "No", or "Not Applicable" - in next column)</i>	Organization's Comments / Explanation
<i>This is a sequence number for identifying the question within the assessment</i>	<i>This is the SHIPM policy number correlating to the topic</i>	<i>This is the title of the SHIPM policy</i>	<i>The requirement related to the SHIPM topic will be included here.</i>	<i>Assessment question will be asked in this field.</i>	<i>This is where the organization will answer the question from the previous column - a drop down list of possible answers will be provided (the drop down list provided is just an example)</i>	<i>The organization may provide additional remarks or information in this field. However, if the organization's answer in the previous column is "Partially" - an explanation in this field is required.</i>
2	2.2.1	Decedents	Health information of decedents must be protected by all the same safeguards as that of living persons.	Has the organization implemented procedures/measures to ensure health information of decedents is protected the same way as that of living persons?	Yes we are fully compliant with the stated requirement (If this response is selected, Organization must provide comment/explanation in "Organization Comments/Explanation" column)	Author wrote and implemented artifact/document prior to original 2003 HIPAA implementation, we are in the process of reviewing and updating all documents related to HIPAA regulations. We expect to complete this review by 12/31/15.

**CalOHII Compliance Program - Review Worksheet Tool**

Responses to be provided in non-shaded area(s)

Agency/Department Information	Agency/Department Response
Agency/Department Name	
Agency/Department Location(s)	
Security Officer Name and Contact Information	
Information Security Officer Name and Contact Information <i>(if different than Security Officer)</i>	
Privacy Officer Name and Contact Information	
Privacy & Security Training Officer / Coordinator Name and Contact Information	
Organization's Breach Response Coordinator Name and Contact Information	
Organization's Response to CalOHII Covered Entity Self Assessment Survey / Date of Response / Responder's Name	
Facility/Location Background	Agency/Department Response
Describe overall business operations <i>(please also describe the populations that you serve)</i>	
How does your Organization create, disclose, receive, store, or use patient health information?	
How many separate departments, programs, or offices are part of your Organization <i>(list all) ?</i>	
How do the above departments, programs or offices create, disclose, receive, store, or use patient health information?	
Please describe the functions and resource allocations <i>(including staff)</i> of your Privacy <u>and</u> Security compliance programs?	
Number of people who work for the department (if you are a Hybrid Entity the number of people working for your HIPAA-covered components) <i>(including interns, contractors, volunteers, temporary employees &amp; all State staff)</i>	
Does your Organization have facilities licensed by the California Department of Public Health (CDPH)? <i>please list</i>	

Compliance Program Sequence #	SHIPM Policy #	SHIPM Topic	Requirement	Organization Question	Organization's Response / Answer <i>(Please provide explanation why you've answered "Yes", "Partially", "No", or "Not Applicable" - in next column)</i>	Organization's Comments / Explanation
1	2.1.1	Authorization for Release of Health Information (A)	Except as otherwise permitted by law, a state entity may not use or disclose health information without a valid authorization. When a state entity obtains or receives a valid authorization for its use or disclosure of health information, such use or disclosure must be consistent with that authorization.	Does the organization have implemented P&Ps regarding the authorization for release of health information?		
2	2.2.1	Decedents	Health information of decedents must be protected by all the same safeguards as that of living persons.	Has the organization implemented procedures/measures to ensure health information of decedents is protected the same way as that of living persons?		
3	2.2.2	Employers	Organizations are permitted to disclose health information to an employer about a member of the employer's workforce for payment for health care services, if there is a valid authorization, or when required by law.	Has the organization implemented procedures/measures to ensure health information is only disclosed to employers when permitted?		
4	2.2.3	Fundraising	A valid authorization must be obtained from the patient prior to using or disclosing health information for fundraising purposes.	Has the organization implemented procedures/measures to ensure that fundraising activities do not use a patient's health information unless there is a valid authorization?		
5	2.2.4	Health Oversight	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.	Has the organization implemented procedures/measures to ensure that health information is used by or disclosed to government agencies only when they are legally authorized to conduct health oversight activities?		
6	2.2.5	Judicial and Administrative Proceedings	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.	Has the organization implemented procedures/measures to ensure that if health information is disclosed for judicial or administrative proceedings without a patient authorization, the organization attempts to notify the patient?		
7	2.2.6	Law Enforcement	Health information may be disclosed, without an authorization from the patient, for law enforcement purposes to law enforcement officials, provided certain conditions are met.	Has the organization implemented procedures/measures to ensure that disclosures for law enforcement purposes meet the required conditions?		
8	2.2.7	Marketing	State entities may not use or disclose a patient's health information for marketing purposes.	Does the organization have written P&Ps regarding marketing activities?		
9	2.2.8	Opportunity to Agree or Object	A state entity may use or disclose health information, provided that the patient is informed in advance of the use or disclosure and has the opportunity to agree or prohibit or restrict the use or disclosure.	Does the organization have written P&Ps regarding opportunity to agree or object to specific uses and disclosures of their health information?		
10	2.2.9	Organ Procurement	A patient's health information may be disclosed, without an authorization, to a coroner, or organ or tissue banks, upon request, for the purpose of facilitating organ, eye, tissue donation or transplantation.	Has the organization implemented procedures/measures to ensure that health information is disclosed for organ procurement?		
11	2.2.10	Public Health Activities	Health information must be disclosed to public health authorities, without a patient's authorization, when required by law.	Has the organization implemented procedures/measures to ensure health information is disclosed to public health authorities only when required by law?		
12	2.2.11	Required by Law / Required Disclosures	Health information must be disclosed when required by state or federal law, and limited to the extent required by law.	Has the organization implemented procedures/measures to ensure that health information, only to the extent necessary, is disclosed when required by law?		
13	2.2.12	Research	A patient's health information may be disclosed without a patient authorization for purposes of research, under the following specific circumstances: 1. If approved by the California Health and Human Services Agency Committee for the Protection of Human Subjects, or if approved by a legally authorized institutional review board (IRC) 2. If the patient's health information has been de-identified	Has the organization implemented procedures/measures to ensure health information is only disclosed for research purposes when permitted by law?		
14	2.2.13	Specialized Government Functions	Health information may be disclosed, without a patient authorization, when the use or disclosure involves, or is related to, the following specialized government functions: 1. Correctional institutions and other law enforcement custodial situations 2. Government programs providing public benefits 3. Government agencies administering a government program providing public benefits 4. Military and veterans activities 5. National security and intelligence activities 6. Protective services for the President and others	Has the organization implemented procedures/measures to ensure health information is disclosed, as permitted by law, for specialized government functions?		
15	2.2.14	Treatment, Payment and Health Care Operations (TPO)	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.	Has the organization implemented procedures/measures to ensure health information is used or disclosed to facilitate TPO, only when it has been collected for the purpose of providing health care services?		
16	2.2.15	Underwriting	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.	Does the organization have written P&Ps regarding underwriting activities?		
17	2.2.16	Victims of Abuse, Neglect, or Domestic Violence	Health information may be disclosed, without the patient's authorization, to a government authority authorized by law to receive reports when it's reasonably believed that the patient is the victim of abuse, neglect, or domestic violence.	Has the organization implemented procedures/measures to ensure health information is only disclosed to a government authority authorized by law when its believed that the patient is a victim of abuse, neglect, or domestic violence?		
18	2.2.17	Health Information Exchange (HIE)	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.	Has the organization implemented procedures/measures to ensure it has entered into a valid written contract/agreement prior to using, disclosing, moving or storing information for HIE purposes?		
19	2.3.1	Genetic Information	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.	Has the organization implemented procedures/measures to ensure that genetic health information is not used by health care plans for underwriting purposes?		
20	2.3.2	HIV/AIDS Information	Develop and implement policies and procedures regarding the collection, use and/or disclosure of public health records containing HIV/AIDS information and HIV/AIDS test results.	Does the organization have written HIV/AIDS information P&Ps, or other appropriate documentation?		
21	2.3.3	Mental Health Records	Mental health records are a type of specially-protected information and may only be used or disclosed as provided by law.	Has the organization implemented procedures/measures to ensure that mental health records are not disclosed, except as expressly authorized by law or an authorization?		
22	2.3.4	Substance Abuse Treatment	Substance abuse treatment records are a type of specially-protected information and may only be used or disclosed as authorized by law or an authorization.	Has the organization implemented procedures/measures to ensure that substance abuse treatment records are not disclosed, except as expressly authorized by law or an authorization?		
23	2.3.5	Developmental Services Records	Developmental service records are a type of specially-protected information and may only be used or disclosed as provided by law.	Has the organization implemented procedures/measures to ensure that developmental service records are not disclosed, except as expressly authorized by law?		
24	2.3.6	Psychotherapy Notes	Psychotherapy notes are a type of specially-protected information and may only be used or disclosed as specifically provided by law.	Has the organization implemented procedures/measures to ensure that psychotherapy notes are not disclosed, except as expressly authorized by law or an authorization?		

Compliance Program Sequence #	SHIPM Policy #	SHIPM Topic	Requirement	Organization Question	Organization's Response / Answer <i>(Please provide explanation why you've answered "Yes", "Partially", "No", or "Not Applicable" - in next column)</i>	Organization's Comments / Explanation
25	2.4.1	Response to Breach and Breach Notification (A)	Following a breach of unsecured health information, state entities must provide notification of the breach to affected individuals, the Secretary, appropriate oversight entities, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.	Does the organization have implemented breach and breach notification P&Ps, or other appropriate documentation?		
26	2.5.1	De-identification	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. Organizations are responsible for understanding requirements for de-identifying health information so it is no longer individually identifiable health information.	Has the organization implemented procedures/measures to ensure that health information has been appropriately de-identified before it is disclosed in compliance with federal and state laws?		
27	2.6.1	Incidental Disclosures	A state entity must reasonably safeguard health information from any intentional or unintentional use or disclosure that is in violation of the of the law. A state entity must reasonably safeguard health information to limit incidental uses or disclosures made related to an otherwise permitted or required use or disclosure.	Does the organization have implemented incidental disclosure P&Ps, or other appropriate documentation?		
28	2.7.1	Minimum Necessary (A)	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.	Has the organization implemented procedures/measures to ensure the use or disclosure of health information, if permitted, is limited to the amount of information necessary to accomplish the intended purpose?		
29	2.8.1	Patient's (personal) Representative	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.	Has the organization implemented procedures/measures to ensure that patient representatives are treated the same as the patient?		
30	2.9.1	Requirements for Telehealth	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.	Does the organization have implemented telehealth P&Ps, or other appropriate documentation?		
31	2.10.1	Multiple Covered Functions (A)	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.	Has the organization implemented procedures/measures to ensure that health information is segregated when an organization has multiple covered functions?		

Compliance Program Sequence #	SHIPM Policy #	Topic	Requirement	Organization Question
32a	3.1.1	Contingency Plan (A)	Establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic health information.	Does the organization have implemented P&Ps, or other appropriate documentation, for responding to an emergency or other occurrence that damages systems containing electronic health information?
32b				If answer to question <b>above</b> is yes, has your organization implemented an inventory for recovery of business critical data required for sustained business operations?
32c				If answer to question <b>above</b> is yes, has your organization analyzed and documented the nature and degree of impact on business operations if any of the critical data resources are not available?
32d				If answer to question <b>above</b> is yes, has your organization established strategies for recovering critical data, resources, or processes?
33	3.1.1	Contingency Plans <i>Applications and Data Criticality Analysis</i>	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 components: - Identifying the steps to safeguarding the state entity's electronic systems and electronic health information. - Identifying the state entity's most vulnerable points with regard to electronic systems and electronic health information. - Identifying the state entity's biggest threats to electronic systems and electronic health information. - 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.	Has the organization assessed the relative criticality of specific applications, and data, in support of other contingency plan components, including all of the components listed in the requirement?
34	3.1.1	Data backup and Storage <i>(during transfer) (A)</i>	Create a retrievable, exact copy of electronic health information (including when needed before movement of equipment).	Has the organization implemented procedures to create a retrievable, exact copy of electronic health information?
35	3.1.1	Data Backup Plan	Establish and implement procedures to create and maintain retrievable exact copies of electronic health information.	Has the organization implemented procedures to create and maintain retrievable exact copies of electronic health information?
36	3.1.1	Disaster Recovery Plan (A)	Establish (and implement if needed) procedures to restore any loss of data.	Has the organization implemented procedures to restore any loss of data?
37	3.1.1	Emergency Mode Operation Plan (A)	Establish (and implement if needed) procedures to enable continuation of critical business processes for protection of the security of electronic health information while operating in emergency mode.	Has the organization implemented procedures to enable continuation of secure critical business processes that ensures the security of electronic health information while operating in emergency mode?
38	3.1.1	Testing and Revision Procedures	Implement procedures for periodic testing and revision of contingency plans.	Has the organization implemented procedures for periodic testing and revision of their contingency plan?
39	3.1.2	Security Incident Procedures (A)	Policies and procedures must be implemented that describe how workforce members are to identify, report, respond, and mitigate security incidents affecting health information.	Does the organization have implemented P&Ps, or other appropriate documentation, to address security incidents, including identification and response to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes?
40	3.1.3	Access Authorization	Implement policies and procedures for granting access to electronic health information (ex, through access to a workstation, transaction, program, process, or other mechanism).	Does the organization have implemented P&Ps, or other appropriate documentation, for granting access (and the levels of access) based on the role of the workforce member?
41	3.1.3	Access Establishment and Modification	Following an organizational risk analysis, information access management policies and procedures must be developed, implemented, and maintained that specify who has access to what specific health information and under what conditions.	Was authority to access health information determined after performing a risk analysis?
42	3.1.3	Isolating Functions	Implement policies and procedures that protect the electronic health information from unauthorized access by the larger organization.	Does the organization have implemented P&Ps (if appropriate), or other appropriate documentation, that demonstrates compliance with segregating electronic health information from access by the larger organization?
43	3.1.4	Information System Activity Review	Implement procedures to regularly review information system activity records, such as audit logs, access reports, and security incident tracking reports.	Has the organization implemented procedures to regularly review records of information system activity?
44	3.1.4	Risk Analysis (A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic health information held by the organization.	Has the organization conducted a thorough assessment of the potential risks and vulnerabilities to electronic health information held by the organization?
45	3.1.4	Security P&Ps (A)	Organizations are required to implement policies and procedures to prevent, detect, contain, and correct security violations.	Does the organization have implemented security P&Ps, or other appropriate documentation, to prevent, detect, contain and correct security violations?
46	3.1.5	Log-in Monitoring	Implement procedures for monitoring log-in attempts and reporting discrepancies.	Does the implemented security and awareness training program include information on how users log onto systems and how they are supposed to manage their passwords?
47	3.1.5	Password Management	Implement procedures for creating, changing, and safeguarding passwords.	Does the implemented security and awareness training program include training workforce members how to safeguard password information?
48a	3.1.5	Protection from Malicious Software	Implement mechanisms to guard against, detect and report malicious software.	Has the organization implemented mechanisms to protect against malicious software?
48b				Does the implemented security and awareness training program include reminders of the organization's security software that is used to protect against malicious software?
49	3.1.5	Security Awareness & Training (A)	Implement a security awareness and training program for all members of its workforce (including management).	Has the organization implemented a security and awareness training program for all members of its workforce?
50	3.1.5	Security Reminders	Implement training program periodic security notifications/reminders.	Does the implemented security and awareness training program include periodic security updates?
51	3.1.6	Security Evaluation (A)	Perform a periodic technical and non-technical evaluation, in response to environmental or operational changes affecting the security of electronic health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.	Has the organization performed a periodic technical evaluation?

52	3.1.7	Verification of Identify <i>Person or Entity Authentication</i>	Implement P&Ps to verify that a person or entity seeking access to electronic health information is actually the one claimed and entitled to access.	Has the organization implemented P&Ps to verify that a person or entity seeking access to electronic protected health information is the one claimed and entitled to access?
53	3.1.8	Authorization and Supervision	Implement P&Ps for the authorization of and supervision of workforce members who work with electronic health information or in locations where it might be accessed.	Has the organization implemented P&Ps for the authorization and supervision of workforce members who work with electronic health information?
54	3.1.8	Termination Procedures	Implement procedures for terminating access to electronic health information when the employment of a workforce member ends, or for other reasons.	Has the organization implemented procedures to terminate workforce members access to electronic health information, as appropriate?
55	3.1.8	Workforce Security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic health information, as provided under Information Access Management, and to prevent those workforce members who do not have approval from obtaining access to electronic health information.	Does the organization have implemented P&Ps, or other appropriate documentation, that ensures authorized workforce members have appropriate access to electronic health information?
56	3.2.1	Access Control	Implement technical policies and procedures for electronic information systems that maintain electronic health information to allow access only to those persons or software programs that have been granted access rights as specified in organization's Information Access Management policies and procedures.	Has the organization implemented technical P&Ps to allow access to only those persons, or software programs, that have been granted access rights?
57	3.2.2	Device and Media Controls	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic health information, into and out of a facility, and the movement of these items within the facility.	Does the organization have implemented P&Ps, or other appropriate documentation, that govern the following: - receipt or removal of device or electronic media - movement of hardware into and out of and within the facility?
58a	3.2.3	Facility Access Controls	Implement policies and procedures to limit physical access to its electronic information systems, and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Does the organization have implemented P&Ps, or other appropriate documentation, that limit physical access to its electronic information systems and the facility or facilities in which they are housed (including access to and use of your facilities and equipment)?
58b				If answer to <b>above</b> is yes, has the organization trained the workforce members in your facility access controls?
58c				If answer to <b>above</b> is yes, does your organization have documentation that describes the issuance of authorization credentials are issued (such as access cards) for the facility where the information system resides?
58d				If answer to <b>above</b> is yes, how does your organization periodically review and approve a facility access control (FAC) list?
58e				If answer to <b>above</b> is yes, how does your organization maintain a current list of workforce members with authorized access to the facility - where the information system is housed?
58f				If answer to <b>above</b> is yes, does your organization have documentation that describes the periodic change of access controls following security events (e.g., when keys are lost, combinations compromised, or individuals are transferred or terminated)?
58g				If answer to <b>above</b> is yes, is there documentation that describes how health information is physically protected from unauthorized access by visitors (if visitors, public or workforce members access the work area)?
58h				If answer to <b>above</b> is yes, has your organization implemented physical access controls at worksites, both during and after work hours?
58i				If answer to <b>above</b> is yes, has your organization identified the vulnerabilities in your current physical security capabilities?
58j				If answer to <b>above</b> is yes, has your organization determined which types of locations require access controls to safeguard electronic health information (such as: data centers, peripheral equipment centers, IT staff offices, workstation locations, and others)?
58k				If answer to <b>above</b> is yes, has the organization implemented procedures/measures that address continued maintenance of security (access control) during a service disruption of the secure access control card system, requiring alternate security measures?
59	3.2.3	Facility Access Controls <i>Access Control and Validation Procedures</i>	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Has the organization implemented procedures that control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision?
60	3.2.3	Facility Access Controls <i>Contingency Operations</i>	Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Has the organization implemented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency?
61	3.2.3	Facility Security Plan <b>(A)</b>	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.	Does the organization have implemented P&Ps, or other appropriate documentation (e.g., a Facility Security Plan), that safeguard the facility and the equipment, from unauthorized physical access, tampering and theft?
62	3.2.3	Maintenance Records	Implement policies and procedures to conduct repairs and modifications to the physical components of a facility which are related to security (ex, hardware, walls, doors and locks).	Does the organization have implemented P&Ps, or other appropriate documentation, regarding conducting repairs and modifications to the physical components of a facility which are related to security?
63	3.2.4	Media Accountability	Maintain a record of the movements of hardware and electronic media and any person responsible for the hardware/media.	Has the organization implemented procedures to maintain a record of hardware and electronic media movements and any person responsible for the hardware/media?
64	3.2.4	Media Disposal <b>(A)</b>	Implement policies and procedures to address the disposal of electronic health information, and/or the hardware or electronic media on which it is stored.	Does the organization have implemented P&Ps, or other appropriate documentation, to address the final disposition of electronic health information, and/or the hardware or electronic media on which it is stored?
65	3.2.4	Media Reuse <b>(A)</b>	Implement procedures for removal of electronic health information from electronic media before the media are made available for re-use.	Has the organization implemented procedures for removal of electronic health information from electronic media before the media are made available for re-use?

66	3.2.4	Workstation Security (A)	Implement physical safeguards for all workstations that access electronic health information, to restrict access to authorized users.	Has the organization implemented physical safeguards on all workstations to restrict access to authorized users?
67	3.2.4	Workstation Use & Security (A)	Implement 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.	Has your organization implemented 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?
68a	3.3.1	Audit Controls	Implement hardware, software, and/or procedural mechanisms that track, record, and examine activity in information systems that contain or use electronic health information.	Has the organization implemented mechanisms that record and examine activity in information systems that contain or use electronic health information?
68b				If answer to question <b>above</b> is yes, does your organization's information system produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, and the identity of any user/subject associated with the event?
68c				If answer to question <b>above</b> is yes, are your organization's current audit, logging, and access control techniques and methods documented?
69	3.3.1	Audit Controls	Implement hardware, software, and/or procedural mechanisms that track, record, and examine activity in information systems that contain or use electronic health information.	Does your organization have documentation that addresses the implementation of hardware, software, and/or procedural mechanisms that track, record and examine activity in systems that contain electronic health information?
70	3.3.1	Audit Controls	Implement hardware, software, and/or procedural mechanisms that track, record, and examine activity in information systems that contain or use electronic health information.	Does your organization have documentation that describes how you coordinate the security audit function with other organizational entities?
71	3.3.2	Encryption (FTP and email over internet)	Implement a mechanism to encrypt electronic health information for FTP and email over internet.	Has the organization implemented mechanisms to encrypt and decrypt electronic health information that is transmitted via File Transfer Protocol (FTP/SFTP) or email over internet?
72	3.3.2	Encryption and Decryption (data at rest)	Implement a mechanism to encrypt and decrypt electronic health information for data at rest.	Has the organization implemented mechanisms to encrypt and decrypt electronic health information?
73a	3.3.3	Access Administration Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Has the organization implemented procedures that terminate an electronic session of a user after a predetermined time of inactivity?
73b				If answer to question <b>above</b> is yes, has your organization implemented procedures for re-authentication after session lockout?
74	3.3.3	Access Administration Emergency Access Procedure (A)	Establish procedures for obtaining necessary electronic health information during an emergency.	Has the organization implemented procedures for obtaining electronic health information during an emergency?
75	3.3.3	Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.	Has the organization implemented procedures to assign a unique name and/or number for identifying and tracking user identity?
76a	3.4.0	Integrity Controls and Implementation Process (A)	Implement policies and procedures to protect electronic health information from improper alteration or destruction. Implement security measures to ensure that electronically transmitted electronic health information is not improperly modified without detection until the information is disposed of.	Has the organization implemented P&Ps to protect electronic health information from improper alteration or destruction?
76b				If answer <b>above</b> is yes, has your organization implemented procedures/measures to ensure that only authorized workforce members can modify electronic health information?
76c				If answer <b>above</b> is yes, has your organization identified and documented those workforce members with the ability to alter or destroy data?
77	3.4.0	Mechanism to Authenticate electronic Health Information	Implement electronic mechanisms to corroborate that electronic health information has not been altered or destroyed in an unauthorized manner.	Has the organization implemented mechanisms to corroborate that electronic health information has not been altered or destroyed in an unauthorized manner?
78a	3.4.0	Transmission Security	Implement technical security measures to guard against unauthorized access to electronic health information that is being transmitted over an electronic communications network.	Has the organization implemented security procedures/measures to guard against unauthorized access to electronic health information that is being transmitted over an electronic communications network?
78b				If answer to <b>above</b> is yes, has your organization trained workforce members in these procedures/measures?
78c				If answer to <b>above</b> is yes, has your organization implemented measures to ensure that electronic health information is not altered during transmission?
78d				If answer to <b>above</b> is yes, has your organization implemented measures to protect electronic health information when it is at rest in your systems and tools?

Compliance Program Sequence #	SHIPM Policy #	Topic	Requirement	Organization Question
79a	4.1.1	Administrative P&Ps	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: <ul style="list-style-type: none"> <li>• Demonstrate compliance with California's SHIPM</li> <li>• Be consistent with the entity's Notice of Privacy Practices</li> <li>• Be compliant with state and federal requirements for use and disclosure of health information, including laws and regulations specific to individual departments</li> <li>• Address any applicable reporting requirements, such as those for abuse, neglect, or communicable disease reporting</li> </ul>	Does the organization have implemented administrative P&Ps, or other appropriate documentation, that demonstrate compliance with the specification?
79b				If answer to <b>above</b> question is yes, has your organization implemented a process for updating P&Ps impacted by changes in federal and state privacy and security laws?
79c				If answer to <b>above</b> question is yes, has your organization implemented a process for updating P&Ps impacted by changes in your own organization's business practices (including weaknesses that have been identified during an organization's risk analysis)?
79d				If answer to <b>above</b> question is yes, please provide the last review and revision date of your P&Ps, training, and forms. Please provide information in the "Assessment Organization's Comments / Explanation" column.
80	4.1.2	Privacy Training (A)	Implement a privacy training program for all members of its workforce (including management). For Hybrid Entities, implement training programs for all members of its workforce (including management) in HIPAA covered components.	Has the organization implemented a privacy training program for all members of its workforce (including management)?
81	4.1.3	Sanctions for Violation	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Covered Entity (CE) or Business Associate (BA).	Does the organization have implemented P&Ps, or other appropriate documentation, that apply appropriate sanctions against workforce members who fail to comply with the organization's security P&Ps?
82a	4.1.4	Staffing: Privacy & Security Officer / Official	Identify the privacy and security official(s) responsible for the development and implementation of the P&Ps required to comply with the Privacy and Security Rules.	Has the organization identified a privacy and security official(s) responsible for the development, implementation, and updating of Privacy and Security P&Ps?
82b				If answer <b>above</b> is yes, is your privacy or security official/officer identified as responsible for administrative, physical, and technical safeguards in your organization?
82c				If answer to <b>above</b> is yes, does the privacy or security official/officer review whether workforce members who handle health information have appropriate access to health information as needed to perform their jobs?
82d				If answer to <b>above</b> is yes, does the privacy or security official/officer have responsibility for compliance with the organization's P&Ps, as well as federal and state laws?
83	4.1.5	Trading Partner Agreements (TPAs) (A)	Establish and characterize a data sharing relationship between two, or more, parties and document the business processes and issues related to the exchange of data for a specific flow.	Has the organization implemented TPAs with its trading partners?
84	4.1.5	TPA Companion Guide (A)	Provide Trading Partners with a companion guide related to EDI exchanges (including information about registration, testing, support, and specific information about control record setup, and discretionary fields).	For the HIPAA transactions you are submitting and/or receiving, do you use/maintain a trading partner companion guide document?
85	4.1.6	Waiver of rights related to HIPAA complaints	A patient always has the right to file a complaint with the federal Secretary of Health and Human Services (HHS) if they believe 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.	Has the organization implemented procedures/measures to ensure a patient is not required to waive this right?
86	4.2.1	Consequence of Non-compliance	Organizations 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.	Has the organization implemented procedures/measures to ensure it supports and cooperates with HHS or other federal or state agency compliance investigation activities?
87	4.3.1	Transactions and Code Sets (TCS) (A)	Utilize the current version of standard transactions for Electronic Data Interchange (EDI) of health care data, including: NCPDP D.0 COB Coordination of Benefits NCPDP D.0 Eligibility for a Health Plan NCPDP 5.1 and NCPDP D.0 Retail Pharmacy Drug Claims NCPDP 3.0 Medicaid Pharmacy Subrogation ASC X12 270/271 Eligibility Benefit Inquiry and Response ASC X12 276/277 Claim Status Inquiry and Response ASC X12 278 Referral Certification and Authorization ASC X12 820 Premium Payment ASC X12 834 Enrollment/Maintenance ASC X12 835 Remittance Advice ASC X12 837 D, P, I Electronic Claims ASC X12 837 COB	Does the organization adhere to the required format <u>and</u> content of standard transactions for any EDI transmission of health care data?
88	4.3.1	TCS - Transactions	Utilize the current version of standard transactions for Electronic Data Interchange (EDI) of health care data.	Do any of the HIPAA transactions you are submitting and/or receiving incorporate "exceptions" from the standard (current version)?
89	4.3.1	TCS - Code Sets	If standard transactions are used for EDI, the organization must use the adopted specific code sets, including: ICD-10-CM HCPCS CPT-IV NDC CDT (ADA Codes)	Does the organization adhere to the standard code sets format <u>and</u> content for EDI transmission of health care data?
90	4.3.1	TCS - Code Sets	If standard transactions are used for EDI, the organization must use the adopted specific code sets.	Do any of the HIPAA code sets you are submitting and/or receiving incorporate "exceptions" from the current standards (e.g., local codes)?
91	4.4.1	Business Associate Contracts (written contract or other arrangement) (A)	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. Document the satisfactory assurances through a written contract or other arrangement with the business associate that meets the applicable requirements.	Does the organization execute Business Associate Agreements (or MOUs) with all Business Associates, and require its Business Associates to have BAAs with its subcontractors, that ensure the Business Associate complies with the organization's P&Ps related to health information and its responsibilities as a Business Associate?
92	4.5.1	Identifiers (provider, health care plan, employers)	Covered health care providers and all health plans and health care clearinghouses must use the approved identifiers in the administrative and financial transactions adopted under HIPAA.	Does the organization adhere to the format and content of the NPI for EDI transmission of health care data via health care transactions?
93	4.6.1	Contractors	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.	Has the organization implemented procedures/measures to ensure that contractors comply with the same requirements and restrictions for health information that apply to the organization (including reporting breach to the covered entity)?
94	4.6.3	Health Information Organizations (HIOs)	HIOs must comply with all of the privacy, security and administrative requirements applicable to business associates 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, business associates and other organizations which will be participating with the HIO to use, disclose, move, or store health information for health information exchange purposes.	If your organization performs services as an HIO or participates with any HIOs, has a valid written contract or other agreement been executed (such as the CalDURSA)?

**Patient Rights - Compliance Program Questions**

<b>Compliance Program Sequence #</b>	<b>SHIPM Policy #</b>	<b>Topic</b>	<b>Requirement</b>	<b>Organization Question</b>	<b>Organization's Response / Answer</b> <i>(Please provide explanation why you've answered "Yes", "Partially", "No", or "Not Applicable" - in next column)</i>
95	5.1.1	Accounting of Disclosures <b>(A)</b>	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 (for those disclosures that must be recorded, tracked, and reported).	Has the organization implemented P&Ps to document, track, maintain information, and provide an accounting of disclosures of health information?	
96	5.2.1	Patient Request to Amend Health Information <b>(A)</b>	The covered entity must permit a patient to request that the covered entity amend the health information maintained in a designated record set.	Does the organization have implemented P&Ps addressing a patients' right to request to amend health information?	
97	5.3.1	Notice of Privacy Practices (NPPs) <b>(A)</b>	A Notice of Privacy Practices (NPP), which reflects the actual privacy practices of the entity, must be posted in a prominent location, must be given to patients of the organization and obtain acknowledgement within the required time limit, and updated as necessary.	Has the organization implemented P&Ps to ensure NPP's are posted in a prominent location, given to patients of the organization and acknowledgement obtained within the required time limit, and updated as necessary?	
98	5.4.1	Patient Access to Health Information	Apply appropriate policies & procedures that allow a patient the right of access to inspect and obtain a copy of their health information in a designated record set, and an Organization's right to deny access, for as long as the health information is maintained in the designated record set (exceptions apply).	Does the organization have implemented P&Ps regarding patient access to their health information maintained in a designated record set, and an Organization's right to deny access?	
99	5.5.1	Restriction for Self-pay	Patients have a right to request privacy protection for health information including the restriction of uses or disclosures of their own health information.	Has the organization implemented procedures/measures to process patients' request for restrictions on the use and disclosure of their own health information if they have self-paid for the services?	
100	5.5.1	Confidential Communications	Patients have a right to request to receive communications by alternative means or at alternative locations.	Has the organization implemented procedures/measures to process requests to receive communications by alternate means or at alternate locations?	

Column	Column Header
<b>A</b>	Compliance Program Sequence #
<b>B</b>	SHIPM Policy #
<b>C</b>	Topic
<b>D</b>	Requirement
<b>E</b>	Organization Question
<b>F</b>	Organization's Response / Answer
<b>G</b>	Organization's Comments / Explanation
<b>H</b>	Was artifact submitted <i>(CalOHII Admin Team to complete)</i>
<b>I</b>	Date of Examination
<b>J</b>	Assigned Assessor Initials
<b>K</b>	Was question/ item examined
<b>L</b>	Which Artifact checklist was utilized during examination?
<b>M</b>	Does document(s) pass CalOHII artifact checklist requirements? <i>(for rows associated with an artifact)</i>

<b>Pick List or Free Form</b>
Pre-Populated
Org Complete
Org Complete
Pick List
Free Form
Pick List
Pick List
Pick List
Pick List

<b>Column</b>
<b>N</b>
<b>O</b>
<b>P</b>
<b>Q</b>
<b>R</b>
<b>S</b>
<b>T</b>
<b>U</b>
<b>V</b>
<b>W</b>
<b>X</b>
<b>Y</b>
<b>NOTE</b>

Column Header
Explanation regarding "Partial"
Does response/artifact/document demonstrate compliance with federal and state laws?
Is this an Area of Concentration during the Organization's onsite visit?
Explanation Regarding Area of Concentration for onsite visit
Is the organization abiding by/enforcing, practicing the documented P&Ps, procedures/measures/required activities?
Does the organization's practices and/or enforcement of these practices, whether documented or not, represent reasonable and appropriate safeguards to comply with the stated requirement?
Assessor's Observations - Free Form (minimum required elements: assessor initials, date, location of observation, name of person meeting with, what was the observation, how did the item either meet or not meet the requirement, what specifically was missing if didn't meet the requirement)
Comments - Free Form (e.g.: memory trigger, special comments, anything you want documented that would be pertinent to the report - must include initials and date, most recent comments to be at the top of the cell)
Overall Findings (related to this question) <b>Note: This applies to "Parent" questions</b>
Recommended Actions - Free Form (minimum required elements: where/what are their missing elements, what they need to do to comply with the legal requirement; please do not include "how")
Compliance Program Manager's Approval
Compliance Program Manager's Comments
For column "V" (Overall Findings) there is a place for a summary of organizational systemic issues, concerns risks ... and strengths. This will be completed/summarized after the findings are completed for each row of a topic (tab).



**Drop Down Answer Lists**

**Policies & Procedures**

Yes

P&Ps are implemented and are complete

Yes

P&Ps are implemented but are incomplete  
(being reviewed and revised)

Yes

P&Ps are implemented but are incomplete  
(out of date, no formal leadership approval, do not contain all  
required elements)

No

P&Ps aren't implemented yet

Not Applicable