

Policies and Procedures – Tips and Tools

Introduction and Background

The California Office of Health Information Integrity (CalOHII) has developed the *Statewide Health Information Policy Manual* (SHIPM) using preemption analysis to ensure compliance with applicable state and federal laws and regulations – the SHIPM references requirements for policies and procedures. Health Insurance Portability and Accountability Act (HIPAA) regulations require covered entities to “Implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements...”¹ To assist departments, CalOHII created a checklist outlining all required policies and procedures – this document can be found in the [SHIPM](#) Chapter 4, 4.1.1 Policies and Procedures.

Additionally, CalOHII requests copies of selected documents to demonstrate compliance during the compliance review process. For a list of the documents requested, refer to the Compliance Review Artifacts Request List which can be found on the CalOHII website ([Compliance Review](#) page).

Several departments have requested additional information on how to develop policies and procedures as well as some examples. CalOHII has compiled this document to assist departments – it contains tips and tools on how to develop policy and procedure documents including how to pull together the applicable information and ideas on how to present or document the information.

Tips and Tools

General:

- **Information in this document must be used in coordination with the SHIPM.**
 - The SHIPM was compiled and developed using preemption analysis and outlines the details of what each policy/procedure must contain to be compliant with applicable state and federal laws and regulations.
 - Required policies and procedures are noted in the “Policy” and/or “Implementation Specifics” sections of the SHIPM.
 - An additional tool for identifying required policies and procedures is the checklist provided in Chapter 4, 4.1.1 Policies and Procedures of the SHIPM.
- As you identify HIPAA required policies and procedures, keep in mind this does not mean new documents must be created – instead, it likely means reviewing

¹ 45 CFR 164.306(b)(2)

Policies and Procedures – Tips and Tools

your current documentation to ensure it addresses HIPAA specific requirements. For example:

- When developing the policies and procedures to ensure compliance with SHIPM, Section 3.3.5 Access Control, you may find that you already have documentation in place as part of your *Operational and Technical Policies and Procedures* required for *Statewide Information Management Manual* (SIMM) 5305 A.² Rather than develop new documentation for HIPAA, review your current *Access Control Policies and Procedures* to ensure compliance with the items outlined in SHIPM sections “Policy” and “Implementation Specifics”. When your review finds items are missing or the document is deficient - update or add the items to your current document. Ensure your document change log is updated to reflect modifications were made for SHIPM compliance (adding the specific SHIPM citation for easy reference).
- Keep in mind, there is no “gold standard” template or format for policies and procedures – it is important to create documents that are useful to the organization to ensure the practices are in place for compliance.
 - Using templates or “boiler plate” documents actually could put the organization at risk for non-compliance during audits if the reviewer/auditor finds the organization does not follow the steps outlined in the documentation.
- CalOHII has published the checklists used during Compliance Reviews – these are helpful when developing policies and procedures to ensure the department is capturing all required elements. Checklists can be found on the CalOHII website ([Compliance Review Artifacts Checklists](#) page).
- Ensure all documentation is kept current and all changes/updates are tracked using a change log – this demonstrates to reviewers and auditors that the organization performs periodic reviews/updates.
 - Incorporate policy and procedure documentation reviews into your project management process – this ensures system or operational changes are assessed for potential HIPAA impacts.
- Ensure all updates are reviewed and approved by management.

Below are links to general information on policy and procedure development as well as ideas for presenting or formatting the information:

- The [Office for Civil Rights \(OCR\)](#) within the U.S. Department of Health and Human Services (HHS) provides a number of tools for HIPAA. This site includes

² State of California ISO. (September 2013). [Information Security Program Management Standard. SIMM 5305-A](#), p. 19

Policies and Procedures – Tips and Tools

an educational series on the HIPAA Security Rule with a topic specific to documentation – “[Organizational, Policies and Procedures and Documentation Requirements.](#)”

Policies:

- Policies define an organization’s values and expected behaviors (the WHAT and WHY) – they establish measurable objectives and expectations for the workforce, assign responsibility for decision making, and define enforcement and consequences for violations³.
- Review the State Administration Manual (SAM) and the SIMM – many times the overall policy for a particular area has been defined by the State. This can serve as a starting point for policy development.
- National Institute of Standards and Technology (NIST) offers detailed information about what system specific policy should address in their [Special Publication \(SP\) 800-14 Generally Accepted Principles and Practices for Security Information Technology Systems](#) – refer to Section 3.1 Policy.

Procedures:

- Procedures describe 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).
- The goal of procedures is a useable document that promotes consistent processes across the organization – this demonstrates consistent compliance to HIPAA regulations.
 - Logs and/or tracking mechanisms supporting the procedures provide evidence of compliance and help the organization demonstrate compliance during reviews or audits.
 - Examples include: logs that track authorizations for the release health information, system logs that indicate consistent security upgrades applied.
- Keep it simple and easy to understand – the language and format should be straight forward. The following provides tips and examples for developing procedure content:
 - Break down the process into step-by-step instructions.
 - How should the process be completed? Define the specific activities and ensure they are in the proper order.
 - When are the activities to be completed?

³ CMS. (2007). [Organizational, Policies and Procedures and Documentation Requirements](#). *Security Rule Educational Paper Series*, p. 6

Policies and Procedures – Tips and Tools

- Where the activities should be completed?
- Document any materials, equipment, or supplies needed.
- Reference applicable laws, regulations or standards to follow.
- Provide templates for logs, forms, communications, reports, etc. to ensure consistency.
- Process flow diagrams or flow charts can help illustrates steps of the procedure.
- Keep the format of procedure documentation consistent across the organization for all procedures created – this helps users know where items can be found across procedures. For example, all procedure documentation has the same sections, in the same order. Such as, each procedure document is broken into the following sections:
 - Policy
 - Procedure – begins with step-by-step, followed by a process flow
 - Templates
 - Cross-reference to other procedures
- All procedure documentation has the same look – same font, headers, etc.

Disclaimer: CalOHII provides departments with this document as a guide, we offer the information which includes some external sources. This list and associated links are not exhaustive. CalOHII does not endorse or validate websites external to CalOHII.