

Risk Analysis – Tips and Tools

Introduction and Background

The *Statewide Health Information Policy Manual* (SHIPM) developed by the California Office of Health Information Integrity (CalOHII) provides an analysis of applicable Federal (including HIPAA) and State laws and regulations related to the Risk Analysis/Assessment - see SHIPM Chapter 3 - 3.1.4 Security Management Process for specific information on the Risk Analysis/Assessment.

The Security Risk Analysis is critical for Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance – it demonstrates and documents the State’s efforts to properly assess the current realm of potential threats to critical information assets (especially those with electronic Protected Health Information or “ePHI”) to determine areas of vulnerability that put these assets (and ePHI) at risk. Additionally, the Risk Analysis provides critical information for ongoing risk management which allows the organization to track, monitor and mitigate critical risks.

HIPAA Privacy and Security compliance at the Federal level is the responsibility of the Office for Civil Rights (OCR). OCR conducts compliance audits and investigates data breaches. As a result of these activities, OCR has consistently found organizations are struggling with the Risk Analysis requirement¹. Many organizations do not have a completed Risk Analysis while others did not complete it properly (i.e., only assess compliance without completing threat/risk assessment). For the few that completed the Risk Analysis, it was not reviewed and updated periodically to reflect current threats/vulnerabilities².

The California Office of Health Information Integrity (CalOHII) has compiled this document to assist California State Departments ensure their Risk Analysis/Assessments are compliant with HIPAA rules. This document contains:

- A comparison of the HIPAA Risk Analysis and the California (CA) Risk Assessment required by the California Chief Information Officer (CA CIO) per the *California State Administration Manual* (Section 1)
- Tips and tools to assist departments with the Risk Analysis/Assessment process (Section 2)

¹ Source: Various news articles on OCR website <http://www.hhs.gov/hipaa/newsroom/index.html>

² Foster Swift Collins and Smith, April 20, 2016, *Recent Seven Figure Settlements Underscore the Importance of HIPAA Compliance*. <http://www.lexology.com/library/detail.aspx?g=188d9998-7491-4481-a516-f71afdd1b4e3>

Risk Analysis – Tips and Tools

Section 1 - HIPAA Risk Analysis versus CA Risk Assessment

There is confusion regarding the HIPAA Risk Analysis³ and the CA Risk Assessment⁴ required under *State Administration Manual (SAM)* – some of the questions raised include:

- Aren't we covering this HIPAA requirement with the CA Risk Assessment?
- Do we need to complete another document for HIPAA compliance?
- How does HIPAA's Risk Analysis compare with or fit into the CA Risk Assessment?
- How does the Security Risk Assessment (SRA) tool on the CA CIO site fit into this process?

The short answer to all of these questions is...the HIPAA Risk Analysis and the CA Risk Assessment requirements and processes are very similar. The CalOHII recommendation is that the CA Risk Assessment format/standards be followed with special attention to the HIPAA Security Rule items to ensure compliance. Additionally, the SHIPM developed by CalOHII provides a preemption analysis of all applicable laws and regulations related to the Risk Analysis/Assessment (see SHIPM Section 3.1.4 – Risk Analysis).

The remainder of this section provides a comparison of the HIPAA and California SAM process/requirements as well as an overview of the basic steps of the Risk Analysis/Assessment process to highlight the additional considerations or items needed for HIPAA Security Rule compliance.

While the HIPAA Security Rule does not have a prescribed methodology or process for the Risk Analysis, OCR authored a paper⁵ to provide guidance on the process. Their process relies heavily on the National Institute of Standards and Technology (NIST) Risk Management⁶ process. A comparison of the OCR Risk Analysis process to the SAM Risk Assessment process is provided below.

³ 45 CFR 164.308(a)(1)(ii)(A) <http://www.hhs.gov/hipaa/for-professionals/security/index.html>

⁴ Office of Information Security. June 2014. 5305.7 Risk Assessment. *State Administration Manual. SAM 5305.7*

⁵ Office for Civil Rights. July 14, 2010. *Guidance on Risk Analysis Requirements under the HIPAA Security Rule.*

<http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>

⁶ National Institute of Standards and Technology. September 2012. *SP800-30 – Risk Management Guide for Information Technology Systems.* http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Risk Analysis – Tips and Tools

Risk Analysis OCR/NIST SP800-30	Risk Assessment SAM 5305.7
Scope of Analysis	#2 - ...with particular emphasis on the applications of information technology that are critical to state entity program operations.
Data Collection	#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.
Identify and Document Potential Threats and Vulnerabilities	#2 - Identification of the threats to which the information assets could be exposed.
Assess Current Security Measures	#3 - Assessment of vulnerabilities, e.g., the points where information assets lack sufficient protection from identified threats
Determine likelihood of Threat Occurrences	#4 - Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of likelihood of such occurrence.
Determine Potential Impact of Threat Occurrence	
Determine the level of risk	
Finalize documentation	#7 - Preparation of 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 measures, the resources necessary for security management and amount of residual risk to be accepted by the state entity.

While the HIPAA Risk Analysis and the CA Risk Assessment processes align, there are some specific considerations and actions that are needed to ensure HIPAA compliance. The basic steps of the Risk Analysis/Assessment process are bulleted below along with highlights regarding the HIPAA Security Rule specific items:

- Identifying information assets.** A key activity in any Risk Analysis/Assessment is to gather a complete inventory of all information assets – both electronic and paper based. Keep in mind, identifying electronic Protected Health Information (ePHI) throughout the organization means tracking the movement of the information from receipt or creation to where it is used, maintained or stored as well as where it may be transmitted or sent. Reviewing processes can help ensure all information assets with ePHI are identified properly. These assets should already be included in the information assets completed for the Risk Assessment per the State Administration Manual (SAM 5305.7) – it may be

Risk Analysis – Tips and Tools

helpful to add a column or indicator to show which assets have ePHI. This will allow special attention to those assets for compliance as well as highlight these items for any compliance reviews performed by CalOHII or audits by the Office for Civil Rights (OCR).

- **Assessing the current realm of threats and vulnerabilities that could put information assets at risk.** Ensure your assessment reviews the organization as a whole to include ePHI/PHI as well as reviews OCR's website and other health industry sites to gather additional information about potential threats. OCR's website provides detailed information about data breaches, which provides valuable insight about potential vulnerabilities.
- **Evaluating the current organizations security measures, safeguards and controls to protect the information assets.** This will mean including the safeguards in the HIPAA Security Rule as part of the assessment. The HIPAA Security Rule contains Administrative, Physical and Technical safeguards and each of these items must be assessed against the current organization. Maintain any notes, tools, or documents used for evaluation to demonstrate compliance.
- **Assessing all vulnerabilities and threats found during the previous steps to determine the likelihood of the occurrence and impact to the organization in order to determine the overall risk level.** Maintain any notes or documents used during your risk assessment to demonstrate compliance.
- **Documenting the results of the risk analysis/assessment.** Use the Risk Analysis checklist to ensure your final report is compliant. The organization is responsible to demonstrate compliance for each step.

Section 2 - Tips and Tools to Assist with Compliance

This section provides various tools/templates and tips for completing the Risk Analysis/Assessment – primarily focused on ePHI and HIPAA compliance. This section begins with general tools/templates before providing specific tips and tools for each step of the Risk Analysis/Assessment process.

General tools/templates for Risk Analysis/Assessment:

- The California Department of Technology Office of Information Security site contains a toolkit for the Risk Assessment process and document <http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp>
- CalOHII Security Tool which includes risk analysis <http://www.ohii.ca.gov/calohi/content.aspx?id=140>

Risk Analysis – Tips and Tools

- OCR provides materials on the Security Rule – including an Educational Paper on *Basics of Risk Analysis and Risk Management*
<http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>
- National Institute of Standards and Technology (NIST) – within the US Department of Commerce – is responsible for developing information security standards for federal agencies.
<https://csrc.nist.gov/publications/sp800>
 - Several Special Publication (SP) papers are applicable to this process:
 - SP800-30 – *Risk Management Guide for Information Technology Systems*
 - SP800-39 – *Managing Risk from Information Systems*
 - SP800-66 – *An Introductory Resource Guide for Implementing HIPAA Security Rule*
 - SP800-100 – specifically Chapter 10 of the *Information Security Handbook* provides information on the Risk Management Framework
 - SP800-115 – *Guide to Technical Aspects of Performing Information Security Assessments*
- Health Information and Management Systems Society (HIMSS) – a private consortium of health care information technology stakeholders.
<http://www.himss.org/>
 - HIMSS Risk Assessment Toolkit – full suite of tools, articles, etc.
<http://www.himss.org/library/healthcare-privacy-security/risk-assessment>
- The Office of National Coordinator for Health Information Technology (ONC) has produced a guide for helping small health care organizations with risk assessment – this document contains a number of questions organizations should ask while assessing security risks.
<https://www.healthit.gov/sites/default/files/small-practice-security-guide-1.pdf>
- Clearwater Compliance is a consulting organization providing several free tools and templates for HIPAA compliance. They offer an on demand overview of *How to Conduct a NIST-based Risk Assessment to Comply with HIPAA and Other Regulations*.
<https://clearwatercompliance.com/hipaa-education/on-demand-videos/nist-based-security-risk-analysis-and-risk-management/>

The following table provides a cross reference of the OCR HIPAA regulations and terms to the State's policies and terms:

Risk Analysis – Tips and Tools


OCR/HIPAA		State of California		
Topic/Term	CFR	Topic/Term	SAM ⁷	SIMM
Security Management	164.308(a)(1)(i)	Information Security Program Management	5305.1	5305-A
Risk Analysis	164.308(a)(1)(ii)(A)	Risk Assessment	5305.7	
Risk Management	164.308(a)(1)(ii)(B)	Risk Management	5305.6	5330-B

⁷ SAM provides a cross reference to applicable NIST publications

Risk Analysis – Tips and Tools

Step 1 - Identifying information assets.


Ensure your current information assets inventory includes any assets where ePHI is stored, received, maintained or transmitted.

<p>Tips</p> 	<ul style="list-style-type: none"> • Include ePHI in all forms of electronic media – such as hard drives, floppy disks, CDs, DVDs, smart cards, thumb drives, PDAs, portable electronic media, cloud computing, smart phones, tablets, workstations, laptops, copy machines that store images, etc. • For Hybrid Entities, ensure your “covered components” are included in the ePHI inventory and assessed for HIPAA compliance. • Keep in mind any data that is transmitted to or from outside organizations or entities. • It is helpful to consider the movement or flow of ePHI information into the department, within the department and outside the department to determine the full scope of information assets with ePHI. • Consider reviewing all processes involving ePHI to ensure associated information assets are identified. • Per NIST (SP800-66, Appendix E) – the scope of the assessment should include “both the physical boundaries” of the department’s location as well as “a logical boundary covering the media containing ePHI, regardless of its location.” • Ensure remote work force and telecommuters are taken into consideration – portable devices such as laptops, removable media, etc. • SAM 5305.5 Information Asset Management Policy requires the inclusion of both electronic and paper information assets.⁸ • The August 2015 State Auditor Report regarding information security recommends information assets inventories identify the asset owners, custodians, and users as well as the importance of each asset to the organization’s mission and programs.⁹
--	---

⁸ Office of Information Security. June 2014. 5305.5 – Information Asset Management. *State Administrative Manual*. [SAM 5305.5](#)


⁹ California State Auditor. August 2015. *Report 2015-611 High Risk Update – Information Security*. <https://www.auditor.ca.gov/pdfs/reports/2015-611.pdf>

Risk Analysis – Tips and Tools


	<ul style="list-style-type: none"> • Add a column to your current information asset inventory to indicate ePHI is created, stored, received, or transmitted. Documentation is essential for compliance reviews. • Bottom line – can you answer the question “Where is ePHI located in our department and how is it stored/moved throughout the organization?”
<p>Tools</p> 	<ul style="list-style-type: none"> • CA Information Security Office SIMM 5305-A contains a detailed description of how to classify and categorize information assets. https://cdt.ca.gov/wp-content/uploads/2018/01/SIMM-5305_A_2018-0108.pdf • HIMSS offers a consolidated tool for the Risk Assessment – the Excel spreadsheet includes tabs for capturing information assets (see tabs Application Inventory and Hardware Inventory). Caution – these tools do not constitute a full and complete Risk Analysis/Assessment. http://www.himss.org/library/healthcare-privacy-security/risk-assessment

Step 2 - Assessing all possible threats and vulnerabilities.

This is an important step in the risk analysis/assessment process – casting a wide net to gather all possible threats and vulnerabilities ensures your department has considered all areas for risk assessment. Some additional research may be needed to ensure HIPAA- related threats and vulnerabilities are captured for consideration.


<p>Tips</p> 	<ul style="list-style-type: none"> • Keeping current on the latest threats is an ongoing task to ensure the risk analysis/assessment is kept up-to-date and helps protect the organization – monitoring intelligence gathered by US-CERT, virus alerts, Office of Inspector General, California ISO, etc. can provide the most current information on threats • Consider internal information from prior risk assessments, audit comments, security requirements, or system security test results (i.e. vulnerability scans) • Reviewing the OCR site for recent breach investigation materials (specifically the Resolution Agreements) can provide better insight on HIPAA ePHI specific threats and vulnerabilities http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
--	--

Risk Analysis – Tips and Tools


<p>Tools</p> 	<ul style="list-style-type: none"> • HIMSS – provides a list of resources regarding various threat, vulnerabilities and malware sites. Many of these resources provide a current listing of the most recent threats/vulnerabilities. http://www.himss.org/library/healthcare-privacy-security/risk-assessment/threats-vulnerabilities • NIST National Vulnerability database https://nvd.nist.gov/ • NIST – SP 800-30 Risk Management Guide for Information Technology Systems <ul style="list-style-type: none"> ○ Appendices D, E, F provide lists of threats and vulnerabilities. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
---	---

Step 3 - Evaluating the current organizations security measures, safeguards and controls.

This is a key component for HIPAA compliance – ensuring the organization’s current security practices and safeguards are reviewed against the HIPAA Security Rule.

<p>Tips</p> 	<ul style="list-style-type: none"> • In addition to reviewing CA CIO checklists, the HIPAA Security Rule must be reviewed to ensure compliance of the organization’s current security safeguards, practices, controls, etc. • The HIPAA Security Rule indicates some items as “addressable” rather than required, however per SAM 5300 all items are considered “required” – refer to SHIPM Section 3.4.1 for more information since this provides a preemptive, consolidated view of applicable laws and regulations. • Document the evaluation/review and keep it with your Risk Assessment/Analysis (see tools for ideas on documentation). • Consider both technical and nontechnical security controls at all places where ePHI is created, received, maintained, processed or transmitted. • Policies and procedures are a key component for demonstrating compliance – further evidence of compliance can be demonstrated with logs and tracking mechanisms.
--	--

Risk Analysis – Tips and Tools



<p>Tools</p> 	<ul style="list-style-type: none"> • HIMSS offers a consolidated tool for the Risk Assessment – the Excel spreadsheet includes tabs for reviewing the HIPAA Security Rule and evaluating compliance across the organization (see tabs Score Card Definitions and Security Score Card) http://www.himss.org/library/healthcare-privacy-security/risk-assessment • NIST SP800-66 (Revision 1) – <i>An Introductory Resource Guide for HIPAA Security Rule</i> - provides detailed information on each of the items within the HIPAA Security Rule, including a description of the item and sample questions to consider for compliance. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf • The Office for Civil Rights (OCR) has released a crosswalk between the HIPAA Security Rule and the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html • Automated tools are available at CalOHII, OCR and NIST websites – the OCR and CalOHII tools are primarily targeted for small/medium private organizations (i.e. providers) while NIST can be tailored for any organization. These tools provide an automated method for assessing each item in the HIPAA Security Rule. Caution – these tools do not constitute a full and complete Risk Analysis/Assessment. <ul style="list-style-type: none"> ○ CalOHII Security Tool http://www.chhs.ca.gov/ohii/Pages/default.aspx ○ OCR Security Risk Assessment Tool https://www.healthit.gov/providers-professionals/security-risk-assessment ○ NIST HIPAA Security Rule Toolkit http://scap.nist.gov/hipaa/
---	---

Step 4 - Collecting all vulnerabilities and threats to determine the likelihood of the occurrence and impact to organization in order to determine the overall risk level.

While this step is consistent for both the HIPAA and CA Risk Assessment/Analysis – keeping an eye on ePHI and related threats or vulnerabilities will assist with HIPAA compliance.


Risk Analysis – Tips and Tools

A general tip on terminology – a VULNERABILITY triggered or exploited by a THREAT equals a RISK.¹⁰

<p>Tips</p> 	<ul style="list-style-type: none"> • Focus on those items that are reasonably anticipated threats. • Document the method used for evaluating the risk level – include the tools used to evaluate high, medium, low impact or likelihood as well as the risk determination scoring. This should be part of the working papers and kept for audit purposes.
<p>Tools</p> 	<ul style="list-style-type: none"> • NIST SP 800-30 Guide for Conducting Risk Assessments provides a standard for evaluating risk http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf • HIMSS offers a consolidated tool for the Risk Assessment – the Excel spreadsheet includes tabs for collecting and assessing risks http://www.himss.org/library/healthcare-privacy-security/risk-assessment


Step 5 - Documenting the results.

HIPAA is focused on ensuring the risks identified as part of this step are moved into the Risk Management process for continued tracking and monitoring.

<p>Tips</p> 	<ul style="list-style-type: none"> • Documenting risks is the starting point – items documented should be moved into the Risk Management process for ongoing tracking and monitoring. This includes creation of the Corrective Action Plan (CAP) to monitor and remedy the identified risks. • Ensure ongoing, periodic reviews of the Risk Analysis/Assessment – especially after large projects or changes to operations or systems. Add a change log to your final deliverable to show when reviews/updates are made, this will help demonstrate ongoing reassessments. • Regardless of the format selected for the final report (see tools below) – keep all working papers to demonstrate a
--	---

¹⁰ CMS. (2007). Basics of Risk Analysis and Risk Management. *Security Rule Educational Paper Series*, p. 4.
<http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>

Risk Analysis – Tips and Tools

	<p>thorough and complete assessment. Working papers include:</p> <ul style="list-style-type: none"> ○ Information/system assets inventory ○ List of threats/vulnerabilities assessed along with the risk level assessment ○ HIPAA Security Rule assessment against current safeguards, practices, etc.
<p>Tools</p> 	<ul style="list-style-type: none"> • CA CIO offers templates for the reports http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp • NIST SP 800-30 Appendix K contains a template for the final report http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf • HIMSS offers a consolidate tool for the Risk Assessment – the Excel spreadsheet includes tabs for collecting and assessing risks (see the Risk Assessment Report tab) http://www.himss.org/library/healthcare-privacy-security/risk-assessment

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.