**Risk Analysis Process – Considerations for Compliance**

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 Risk Analysis/Assessment - *see SHIPM Chapter 3 - 3.1.4 Security Management Process* for specific information on Risk Analysis/Assessment.

The basic steps of the Risk Analysis/Assessment process are bulleted below highlighting specific considerations for compliance:

* **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 Administrative Manual (SAM § 5305.7) – it may be 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. Additionally, review the California Office of Information Security (OIS) and/or 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 checklist below to help ensure your final report is compliant. The organization is responsible to demonstrate compliance for each step.

For additional information on the Risk Analysis/Assessment process, refer to the Risk Analysis – Tips and Tools document on the CalOHII website.

**Checklist for Compliance**

After completing your Risk Analysis (Assessment), use the following checklist to self-assess your department’s compliance. It is recommended that you print and retain the completed checklist with your Risk Assessment.

| **#** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
|  | Have you identified the PHI (both paper and electronic) within your department and included those assets in your information asset inventory? |  |  |
|  | Do you have documentation demonstrating your review of the organization’s security measures? |  |  |
|  | Do you have documentation of all threats and vulnerabilities gathered, considered and evaluated during the Assessment? |  |  |
|  | Have the risks reported in the Assessment been incorporated into the Department’s ongoing risk management process for tracking, monitoring and resolution? |  |  |
|  | Have you added (or updated) a change log or another tool to demonstrate ongoing and periodic reviews/updates to the Assessment? |  |  |

In addition to the checklist above, the following sites provide other useful tools for assessing compliance:

* CalOHII conducts compliance reviews of California state entities, impacted by HIPAA, to identify any gaps in compliance, ensure corrective action, and to adopt best practices – the Compliance Review checklists are available on the CalOHII website.
* The OCR Audit Program reviews the policies and procedures adopted and employed by covered entities and their business associates to meet standards and implementation specifications of the Privacy, Security, and Breach Notification Rules – their [audit protocol](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html) provides a good reference.