**Statewide Health Information Policy Manual (SHIPM) 2.4.1 – Breach and Breach Notification**

*Compliance Review Tool Question #25*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Was a **Breach P&P** submitted for review?  | Y🞏 N🞏 |  |
| 2 | Does the artifact(s) address the following: |  |  |
| 2a | * How the organization’s workforce can / should recognize a possible Breach and how they are to report it internally (including timelines)?
 | Y🞏 N🞏 |  |
| 2b | * Once reported, how is the Breach (Incident) received and documented?
	+ Reported By (and contact info)
	+ Date and Time Report Received
	+ Date and Time of Breach (Incident)
	+ Date and Time Breach Discovered
	+ Location / Department / Building
	+ Source / Media (e.g., EHR, Paper, Fax, etc.)
 | Y🞏 N🞏 |  |
| 3 | Does the artifact(s) address the following regarding **Breach Investigation:** |  |  |
| 3a | * Include a requirement to complete a Risk Assessment to determine potential harm, and root-cause & corrective actions (*e.g., HIPAA COW Breach Notification Policy – Risk Assessment Tool, NCHICA HITECH Breach Notification Assessment Tool*)?
 | Y🞏 N🞏 |  |
| 3b | * Include a description of the Breach (Incident)?

*May need to include name of Individual(s) involved, Health Information, How and Why the Breach Happened, etc.* | Y🞏 N🞏 |  |
| 3c | * Include / require Privacy Breach Investigation Record / Documentation be created?
 | Y🞏 N🞏 |  |
| 3d | * Include / require a request for the Original(s) / Media to be returned or destroyed with Written Verification of such (if appropriate)?
 | Y🞏 N🞏 |  |
| 3e | * Include instructions on the possibility of initiating a Security Incident process (if applicable)?
 | Y🞏 N🞏 |  |
| 3f | * Include the steps to determine whether there was Business Associate (BA) / Vendor Involvement?

*May need to locate signed BA agreement, if no BA agreement with Vendor document why not* | Y🞏 N🞏 |  |
| 3g | * Include a recommendation to assess/engage need for Forensics (*as appropriate*)?
 | Y🞏 N🞏 |  |
| 3h | * Include a recommendation to assess/engage need for Private Investigator (*as appropriate*) (*e.g., research Craigslist, eBay, etc. for stolen equipment*)?
 | Y🞏 N🞏 |  |
| 4 | Does the artifact(s) address the following regarding **Notifications and Reporting:** |  |  |
| 4a | * The Internal notifications (as appropriate)?
	+ IT Leadership
	+ Risk Management, Compliance Officer, Human Resources, Leadership, etc.
	+ Internal Legal Counsel
	+ Public Relations & Communication(s) / Customer Service
	+ Building Services / Facilities

*May need to create an immediate script for Response to / for incoming inquiries about the Breach*  | Y🞏 N🞏 |  |
| 4b | * The **required** External notifications/reporting?
	+ HHS
	+ DOJ
	+ OIS/CHP (via Cal-CSIRS)
	+ CalOHII
 | Y🞏 N🞏 |  |
| 4c | * *Conditional* External notifications (*if appropriate*)?
	+ External Legal Counsel
	+ Law Enforcement Officials (based on geographic location and nature of crime)
	+ Insurance Carrier (e.g., Facility, Cyber, Malpractice, etc.)
	+ Individuals (patients)

*Including Date, Time, Agency and Names of Individuals Breach info shared with* | Y🞏 N🞏 |  |
| 4d | * Describe the Office of Civil Rights Notifications requirements including:
	+ <500 Individuals
		- Notify OCR within reasonable time period or <60 days
	+ >500 Individuals
		- Notify OCR within reasonable time period or <60 days
		- Notify Individuals
		- Notify Medical Outlets

*May need to consult with Senior Leadership, Legal Counsel, Business Unit Leader* | Y🞏 N🞏 |  |
| 4e | * If organization is a Health Plan, Provider of Health Care or Facility, does it describe State and / or Federal Agency(s) requirements (if required) (e.g., Health Plans with Medicare Plans – Contact CMS)?
 | Y🞏 N🞏 |  |
| 5 | Does the artifact(s) address the following regarding **Breach Mitigation / Follow-up Activities** |  |  |
| 5a | * ***Communication Plan*** – to cover oral, electronic and written communications to Victims, as well as information to assist with Personal Needs
 | Y🞏 N🞏 |  |
| 5b | * Report to Senior Leadership
 | Y🞏 N🞏 |  |
| 5c | * Completion of Breach Investigation Report
 | Y🞏 N🞏 |  |
| 5d | * Record disclosure information in Accounting of Disclosure records
 | Y🞏 N🞏 |  |
| 5e | * Require completed Breach checklist (and other supporting breach investigation records) are retained for six years
 | Y🞏 N🞏 |  |
| 5f | * Completion of Workforce member Sanctions (as applicable / appropriate)
 | Y🞏 N🞏 |  |
| 5g | * ***Business Associate*** – Request BAs mitigation plan, BA responsibilities for breach management, and documentation of steps on how the BA will ensure the event does not reoccur (as applicable / appropriate)
 | Y🞏 N🞏 |  |
| 5h | * Consideration of External Vendor specializing in Breach Notification (*e.g., Cyber-Insurance vendor*) (*as applicable / appropriate*)
 | Y🞏 N🞏 |  |
| 5i | * Consideration of External vendor specializing in Credit Card Monitoring (*as applicable / appropriate*)
 | Y🞏 N🞏 |  |
| 5j | * ***Communication to Workforce*** – Learning Opportunity (*e.g., newsletter article, meeting, presentation, etc.*) (*as applicable / appropriate*)
 | Y🞏 N🞏 |  |
| 6 | Does the artifact(s) describe the required Content elements of a **Breach Notification** to Individuals (patients)? |  |  |
| 6a | * Written in plain language and titled “**Notice of Data Breach**”, with titles and heading clearly and conspicuously displayed in font no smaller than 12-point type?
 | Y🞏 N🞏 |  |
| 6b | * Titled “**What Happened**”, provide a brief description of what happened (*if that information is possible to determine at the time the notice is provided*), including:
 | Y🞏 N🞏 |  |
|  | * + Date of the breach (or estimated date, or the date range within which the breach occurred)
	+ Date of the discovery of the breach
	+ Whether the notification was delayed as a result of a law enforcement investigation
	+ Date of the Notice
 | Y🞏 N🞏 |  |
| 6c | * Titled “**What Information Was Involved**”, provide a description of the types of unencrypted / unsecured health information involved in the breach
 | Y🞏 N🞏 |  |
| 6d | * Titled “**What you Can Do**”, provide advice on any steps individuals should take to protect themselves from potential harm resulting from the breach.
 | Y🞏 N🞏 |  |
| 6e | * + Also, provide the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, driver’s license number, or California identification card number
 | Y🞏 N🞏 |  |
| 6f | * Titled “**What We Are Doing**” provide a brief description of what the state entity is doing to investigate the breach, to mitigate harm to the patients, and to protect against further breaches.
 | Y🞏 N🞏 |  |
| 6g | * Titled “**For More Information**”, provide the name and contact information of the reporting state entity
 | Y🞏 N🞏 |  |
| 6h | * If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed health information
 | Y🞏 N🞏 |  |
| 7 | Does the artifact(s) describe the required Timing of the **Notification(s)** per SHIPM 2.4.1, III. G? | Y🞏 N🞏 |  |
| 8 | Does the artifact(s) describe the required Methods of **Notification(s)** (*including alternate methods*) per SHIPM 2.4.1, III. E? | Y🞏 N🞏 |  |
| 9 | Does the artifact(s) have official review/acceptance? |  |  |
| 9a | * Effective Date
 | Y🞏 N🞏 |  |
| 9b | * Revision Date
 | Y🞏 N🞏 |  |
| 9c | * Authorizing Sr./Executive Management Signature
 | Y🞏 N🞏 |  |

Title(s) of Submitted Policy/Document/Artifact(s) Reviewed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Stored Location of, or link to Artifact(s) Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Overall CalOHII Reviewer Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of CalOHII Reviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_

Title of or link to Other Source(s) used (e.g., sources not in checklist, templates) – *optional*:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/>