**Statewide Health Information Policy Manual (SHIPM) 3.1.5 – Security Awareness and Training**

*Compliance Review Tool Questions #49 and 50*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact(s) regarding their Security Awareness and Training procedures? |  |  |
| 2 | Does the artifact(s) describe that all workforce members begiven security training regarding the organization’s security policies and procedures, as follows: | n/a |  |
| 2a | * Is training provided to each **new** workforce member within a reasonable period of time after the person joins the workforce and ***prior to accessing health information*?** |  |  |
| 2b | * Is training updated and provided within a reasonable period of time after a material change in the policies and procedures becomes effective? |  |  |
| 2c | * Is training documented in writing, which may be an electronic training record, and include which workforce members were trained, topics covered, and training dates? |  |  |
| 2d | * Does the training establish rules of conduct and instruct each workforce member about the rules and procedures concerning security? |  |  |
| 3 | Does the security awareness and training reflect the organization’s security policies and procedures about all the following topics: | n/a |  |
| 3a | * Are there periodic security updates to remind workforce members of their role in protecting health information (*e.g., discussion topics at monthly meetings, focused reminders posted in affected areas, banner reminders*)? |  |  |
| 3b | * Is there subject matter for protection from malicious software (*e.g., unauthorized downloads from the Internet, opening email attachments from unknown senders, etc.*)? |  |  |
| 3c | * Is there subject matter for Log-in monitoring (*e.g., the procedures for monitoring log-in attempts and reporting discrepancies – the purpose is to make workforce members aware of log-in attempts that are not appropriate*)? |  |  |
| 3d | * Is there subject matter for Password management – creating, changing and safeguarding (*e.g., prevent the sharing of passwords, not leaving written passwords in areas that are visible or accessible to others, etc*.)? |  |  |
| 4 | Does the artifact(s) document periodic security retraining for ongoing awareness based on operational changes, technology updates, and security risks  (*should be conducted as needed and at least annually*)? |  |  |
| 5 | Does the artifact(s) reflect that the organization document the security reminders they implement? |  |  |
| 5a | * Does the documentation include the type of reminder, its message and the date it was implemented? |  |  |
| 6 | Does the artifact(s) reflect that the organization retain the security awareness and documentation for six years from the date of its creation, or the date when it last was in effect, whichever is later? |  |  |
| 7 | Does the training tracking documentation and/or training logs (*tracking of workforce by individual*), at a minimum, include the following: | n/a |  |
| 7a | * Training Date? |  |  |
| 7b | * Participant Name? |  |  |
| 7c | * Course name? |  |  |
| 8 | Does the artifact(s) have official review/acceptance: |  |  |
| 8a | * Effective Date? |  |  |
| 8b | * Revision Date? |  |  |
| 8c | * Document the authorizing (senior or executive) management approval? |  |  |

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

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

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

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

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

Overall CDII Reviewer Comments:

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

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

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

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

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

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

CalHHS/OCR provides [training materials](https://www.hhs.gov/hipaa/for-professionals/training/index.html) to assist with the implementation of privacy/security training, the materials can be found at the following link:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/training