Note: if your response for a requested artifact references a separate document such as a supporting policy or procedure, provide a copy of the additional documentation or it may be considered non-compliant.   
For additional help - refer to the last five (5) columns to the right of each artifact item and/or the [Tips and Tools section](https://www.chhs.ca.gov/ohii/compliance-review/#tips) of the Compliance Review Program page on the CalOHII website.

| **#** | **Checklist** | **Title** | **Description** | **Compliance Review Tool Tab Name** | **Compliance Review Tool Question #** | **SHIPM Policy #** | **SHIPM Topic** | **Checklist Name** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** |  | Authorizations for Disclosure (a) | ​Documentation of organization's policies and procedures for Authorizations for the Release of Health Information (PHI/ePHI), describing both **what** the organization does, and **how** the organization complies with the requirements to allow and accept Authorizations for Disclosure from the individual/patient (including an explanation of the process utilized to determine whether the Authorization is valid - that it contains the required elements, and how organization staff would access such tracking).  *This should be enterprise-level documentation and/or desk level reference documentation (such as desk guides) - or electronic equivalent. If electronic, please save as soft copy and include with your response.* | Privacy | 1 | 2.1.1 | Authorizations | Authorizations |
| **2** |  | Authorizations for Disclosure (b) | Provide copies of the following:   1. The organization's Authorization tracking log/report, and 2. The organization's most recent Authorization for Disclosure of Health Information (PHI/ePHI). | Privacy | 1 | 2.1.1 | Authorizations | Authorizations |
| **3** |  | Breach Documentation and Log (a) | Documentation of organization's policies and procedures, describing both **what** the organization does, and **how** the organization complies with the requirements to define the breach response related to how the breach is initially reported, tracked, investigated, processed through closure.  *This should be enterprise-level documentation and/or desk level reference documentation (such as desk guides) - or electronic equivalent. If electronic, please save as soft copy and include with your response.* | Privacy | 25 | 2.4.1 | Breach and Breach Notification | Breach Notification |
| **4** |  | Breach Documentation and Log (b) | A list of **all** the organization's breach(s) that have occurred in the most recent 12 month period. The list or log should include (*at a minimum*) the following information:   * Date of event, * Date discovered, * Brief description of breach/suspected breach, * Whether a risk analysis was conducted, * Brief description of result of risk analysis, corrective action plan, and mitigation, * Was it a confirmed breach, * Were notifications sent, * Date of notification, * How many individuals notification sent, and * Reason for delay in notification (if any). | Privacy | 25 | 2.4.1 | Breach and Breach Notification | Breach Notification |
| **5** |  | Breach Notification (a) | ​Documentation regarding the process/procedures/steps the organization follows regarding breach notifications and reporting. For example, how affected patients are notified, as well as all internal and external stakeholders (such as Cal-CSIRS, media, Secretary of Health and Human Services, etc.) | Privacy | 25 | 2.4.1 | Breach and Breach Notification | Breach Notification |
| **6** |  | Breach Notification (b) | A copy of the organization's breach notification (also known as patient notification) related to the most recent breach activity (*if any*), or a template for breach notification, or both. | Privacy | 25 | 2.4.1 | Breach and Breach Notification | Breach Notification |
| **7** |  | Business Associate Agreement (a) | Provide the following:   1. A copy of the organization's BAA template, 2. A recently executed BAA your organization has initiated, and 3. A BAA your organization has recently entered into as a Business Associate. | Administrative | 91 | 4.4.1 | Business Associate Agreement | Business Associate Agreement |
| **8** |  | Business Associate Agreement (b) | ​Documentation that describes **how** the organization will conduct oversight of the Business Associate to ensure they comply with requirements outlined in the BAA, MOU or IA. | Administrative | 92 | 4.4.2 | Oversight of Business Associates | Business Associate Oversight |
| **9** |  | Business Associate Agreement (c) | List of all the organization's BAA contracts and the dates associated with the contracting terms. | Administrative | 92 | 4.4.2 | Oversight of Business Associates | Business Associate Oversight |
| **10** |  | Contingency Plan / Business Continuity Plan  *(also referred to as Emergency Mode of Operation Plan*) | Documentation that demonstrates the organization complies with policies and procedures requirements, specifying **how** to continue critical business practices for the protection of Health Information (PHI/ePHI) while operating in an emergency mode. Provide the following:   1. Created and implemented plans, 2. Documentation of periodic testing results, and 3. Corrective actions to address any issues/gaps. | Security | 32 36 | 3.1.1 | Contingency Plans | Contingency Plan - Business Continuity Plan |
| **11** |  | Contingency Plan / Technology Recovery Plan  *(also referred to as Disaster Recovery Plan*) | Documentation that demonstrates the organization complies with policies and procedures requirements, specifying **how** to respond to an emergency, or other unexpected occurrences, that may damage systems containing Health Information (PHI/ePHI). Provide the following:   1. Created and implemented plans, 2. Documentation of periodic testing results, and 3. Corrective actions to address any issues/gaps. | Security | 32  33 | 3.1.1 | Contingency Plans | Contingency Plan - Technology Recovery Plan |
| **12** |  | Contingency Plan /  Data Backup Plan | ​Documentation that demonstrates the organization complies with policies and procedures requirements, specifying **how** datasets containing electronic Health Information (ePHI) are backed up including associated restoration steps (e.g., *checklists, schedules, prioritization, etc.).* | Security | 35 | 3.1.1 | Contingency Plans | Contingency Plan - Data Backup Plan |
| **13** |  | Device and Media Controls | ​Documentation of organization's policies and procedures describing both **what** the organization does, and **how** the organization complies with the requirements to describe how devices and media containing Health Information (PHI/ePHI) are handled (the processes organization uses to receive, store, wipe *clean*, destroy, and account for, etc.). | Security | 53 54 55  56 | 3.2.2 | Device and Media Controls | Device and Media Controls |
| **14** |  | Facility Security Plan  (*Safeguards*) | Documentation of organization's implemented procedures that describes **how** to safeguard the facility(s) and the equipment within the facility from unauthorized physical access, tampering, and theft. | Security | 60 | 3.2.3 | Facility Access Controls | Facility Security Plan |
| **15** |  | Health Information (PHI/ePHI) locations | ​Documentation or inventory of Health Information (PHI/ePHI) locations within the organization's system and applications (including the flow of Health Information). *Examples of documentation includes: logical or physical data mapping.* | Security | 44 | 3.1.4 | Security Management Process | Health Information Locations |
| **16** |  | Incident Reporting | ​Documentation of the organization's implemented policies and procedures describing both **what** the organization does, and **how** the organization complies with the requirements regarding security incidents. Additionally, the processes/procedures that defines a security incident, describes **how** the organization's workforce reports security incidents, and **how** the organization responds, tracks, mitigates and resolves the incident.  *This should be enterprise-level documentation and/or desk level reference documentation (such as desk guides) - or electronic equivalent. If electronic, please save as soft copy and include with your response.* | Security | 38 | 3.1.2 | Incident Procedures | Incident Reporting |
| **17** |  | Notice of Privacy Practices (NPP) | Provide a copy of the organization's NPP (the document that would be provided to a patient, consumer, subscriber, etc.) | Patient Rights | 99 | 5.3.1 | Notice of Privacy Practices | NPP |
| **18** |  | Patient's (*Individual's*) Right to Access Health Information | ​Documentation of organization's policies and procedures, or information describing both **what** the organization does, and **how** the organization complies with the requirements to allow patient's access to their Health Information (including how the organization receives, tracks, accesses, and processes such requests - including denials and appeals).  *This should be enterprise-level documentation and/or desk level reference documentation (such as desk guides) - or electronic equivalent. If electronic, please save as soft copy and include with your response.* | Patient Rights | 100 | 5.4.1 | Patient's (Individual's) Right to Access Health Information | Individuals Right to Access Health Information |
| **19** |  | Patient's (*Individual's*) Right to Amend Medical Records | Documentation of organization's policies and procedures, or information describing both **what** the organization does, and **how** the organization complies with the requirements to allow patients to amend their Medical Record(s) (including how the organization receives, tracks, accesses, and processes such requests - including denials and appeals).  *This should be enterprise-level documentation and/or desk level reference documentation (such as desk guides) - or electronic equivalent. If electronic, please save as soft copy and include with your response.* | Patient Rights | 98 | 5.2.1 | Patient's (Individual's) Right to Amend Medical Records | Individuals Right to Amend Medical Records |
| **20** |  | Privacy Training Documentation and Tracking | Documentation regarding the organization's implementation of privacy training - this includes:   1. Documentation defining the training program/requirements, to include **how** training is delivered, tracked, and maintained, 2. Copy of the current privacy training materials, and 3. Copy of training tracking logs. | Administrative | 80 | 4.1.2 | Privacy Training | Privacy Training |
| **21** |  | Security Awareness and Training | Documentation regarding the organization's implementation of security awareness and training - this includes:   1. Documentation defining the security awareness and training program, to include **how** training is delivered, tracked and maintained, 2. Copy of the current security training materials, 3. Copies of recent security reminders, and 4. Copy of training and awareness tracking logs. | Security | 49 50 | 3.1.5 | Security Awareness and Training | Security Awareness and Training |
| **22** |  | Security Evaluation(s) | Documentation regarding the organization's most recent:   1. Technical evaluation (such as a network scan or security rule evaluation), and 2. Non-technical evaluation (such as legal, policy, standards, and procedure compliance). | Security | 51 | 3.1.6 | Security Evaluations | Security Evaluations |
| **23** |  | Security Management Process - Risk Assessment / Analysis (a) | Provide a copy of the organization's policies and procedures, or information describing both **what** the organization does, and **how** the organization complies with the requirements to assess potential risks and threats to Health Information (PHI/ePHI). | Security | 43.1 43.2 43.3 | 3.1.4 | Security Management Process | Risk Assessment P-Ps |
| **24** |  | Security Management Process - Risk Assessment / Analysis (b) | Documentation regarding the organization's most recent:   1. Risk assessment(s) (e.g., Report) - including, but not limited to - the identified threats, vulnerabilities, risks, risk tolerance, existing controls and additional controls required to eliminate or mitigate risk, etc. 2. Enterprise-wide POAM - this document includes all corrective actions captured by the organization during their Continuity Plan, Business Continuity Plan, Disaster Recovery Plan, Technology Recovery Plan, Department of Military scans, CalOHII CAP items, etc. | Security | 43.1 43.2 43.3 | 3.1.4 | Security Management Process | Risk Assessment |
| **25** |  | List of Privacy Policies and Procedures | ​Provide a listing of all existing (current) organization Privacy policies and procedures and plans. At a minimum, this list should address the SHIPM required policies and procedures, as well as any SAM required policies and procedures.   *This is only a request for a list, not the actual document(s).* | Privacy | 79.1 79.2 79.3 79.4 | 4.1.1 | Policies and Procedures | n/a |
| **26** |  | List of Security Policies and Procedures | ​Provide a listing of all existing (current) organization Security policies and procedures and plans. At a minimum, this list should address the SHIPM required policies and procedures, as well as any SAM required policies and procedures.   *This is only a request for a list, not the actual document(s).* | Security | n/a | 3.4.1 | Documentation | n/a |
| **27** |  | Organization Chart | Provide a copy of the most current organization chart to the division management level. | n/a | n/a | n/a | n/a |  |