SHIPM Required Policies and Procedures 

The following provides a list of all SHIPM required policy and/or procedure documentation. NOTE: Policy and procedure documentation can be incorporated into existing documentation or as stand-alone documents. Or, if the topic is not applicable to your organization based on your business practices, your organization can create a letter/memo signed by the Privacy Officer or Information Security Officer listing the topics not applicable to the state entity with an explanation why.

| **SHIPM Section** | **SHIPM Policy** | **SHIPM Policy Reference Requirement[[1]](#footnote-1)** | **Completed?** |
| --- | --- | --- | --- |
| 2.1.0 – Authorizations  | 2.1.1 – Authorizations | III. State entities are required to develop, implement, and maintain policies and procedures outlining authorization requirements (when a patient authorization is needed and what must be included). |  |
| 2.2.0 – Uses and Disclosures | 2.2.1 – Decedents | III. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) utilized to safeguard health information of decedents. |  |
| 2.2.0 – Uses and Disclosures | 2.2.2 – Employers  | III. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) utilized to ensure the minimum amount of health information is disclosed to an employer only with a valid authorization. |  |
| 2.2.0 – Uses and Disclosures | 2.2.3 – Fundraising  | III.A. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) used to prevent fundraising activities without a valid authorization. |  |
| 2.2.0 – Uses and Disclosures | 2.2.4 – Health Oversight | III. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information to government agencies performing health oversight activities.  |  |
| 2.2.0 – Uses and Disclosures | 2.2.5 – Judicial and Administrative Proceedings  | III. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information related to a judicial or administrative proceeding.  |  |
| 2.2.0 – Uses and Disclosures | 2.2.6 – Law Enforcement | III. While not specifically required by law, CDII requires state entities to develop, implement, and maintain policies and procedures describing the measures and processes (what and how) related to the use and disclosure of health information for law enforcement purposes.  |  |
| 2.2.0 – Uses and Disclosures | 2.2.7 – Marketing  | III. A. Enforcement entities are responsible for maintaining policies and procedures that outline the details and restrictions of marketing activities.  |  |
| 2.2.0 – Uses and Disclosures | 2.2.8 – Opportunity to Agree or Object  | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to allow patients the opportunity to agree, or object to specific uses and disclosures of their health information. |  |
| 2.2.0 – Uses and Disclosures | 2.2.9 – Organ Procurement | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose a deceased patient’s health information for organ procurement. |  |
| 2.2.0 – Uses and Disclosures | 2.2.10 – Public Health Activities  | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information for public health activities. |  |
| 2.2.0 – Uses and Disclosures | 2.2.11 – Required by Law and Required Disclosures | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information when required or mandated by law. |  |
| 2.2.0 – Uses and Disclosures | 2.2.12 – Research  | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for research purposes. |  |
| 2.2.0 – Uses and Disclosures | 2.2.13 – Specialized Government Functions | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information for specialized government functions. |  |
| 2.2.0 – Uses and Disclosures | 2.2.14 – Treatment, Payment and Health Care Operations (TPO)  | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for TPO. |  |
| 2.2.0 – Uses and Disclosures | 2.2.15 - Underwriting  | III. State entities that are business associates, health care clearinghouses, health care plans, health care providers, or hybrid entities must implement policies and procedures to limit the health information disclosed to the amount reasonably necessary to achieve the purpose for the disclosure.  |  |
| 2.2.0 – Uses and Disclosures | 2.2.16 – Victims of Abuse, Neglect, or Domestic Violence | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information related to victims of abuse, neglect, or domestic violence. |  |
| 2.2.0 – Uses and Disclosures | 2.2.17 – Health Information Exchange (HIE) | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose health information for HIE purposes. |  |
| 2.3.0 – Specially Protected Information | 2.3.1 – Genetic Information | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose genetic health information. |  |
| 2.3.0 – Specially Protected Information | 2.3.2 – HIV/AIDS Information  | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose HIV/AIDS information and test results. |  |
| 2.3.0 – Specially Protected Information | 2.3.3 – Mental Health Records | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose mental health information. |  |
| 2.3.0 – Specially Protected Information | 2.3.4 – Substance Use Disorder Treatment | III.A. State entities must have in place formal policies and procedures to reasonably protect against unauthorized use and disclosure of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information. |  |
| 2.3.0 – Specially Protected Information | 2.3.5 – Developmental Services Records | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose developmental service records. |  |
| 2.3.0 – Specially Protected Information | 2.3.6 – Psychotherapy Notes | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to use or disclose psychotherapy notes. |  |
| 2.4.0 Breach and Breach Notification | 2.4.1 – Breach and Breach Notification  | III. A. Policies and procedures must be developed, implemented, and maintained, to ensure compliance with legal requirements regarding identifying, investigating and reporting breaches or unauthorized disclosures of health information |  |
| 2.5.0 – De-identification | 2.5.1 – De-identification | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to de-identify health information. |  |
| 2.6.0 – Incidental Disclosures  | 2.6.1 – Incidental Disclosures  | III. A. State entities are responsible to develop and implement policies and procedures that require their workforce to limit and prevent disclosures of health information. When those disclosures are incidental to a permitted or required use or disclosure, it does not apply to impermissible uses or disclosures. |  |
| 2.7.0 – Minimum Necessary | 2.7.1 – Minimum Necessary | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to limit disclosure of health information to the minimum necessary. |  |
| 2.8.0 – Patient’s (Personal) Representative | 2.8.1 – Patient’s (Personal) Representative | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to disclose health information to a patient’s representative. |  |
| 2.9.0 – Requirements for Telehealth  | 2.9.1 – Requirements for Telehealth  | II. Health care providers using telehealth to deliver health care services are responsible for implementing and maintaining security and privacy policies and procedures that address the unique circumstances involved in providing telehealth services. |  |
| 2.10.0 – Multiple Covered Functions | 2.10.1 – Multiple Covered Functions | III. While not specifically required by law, CDII requires state entities to develop, implement and maintain policies and procedures describing the measures and processes (what and how) utilized to ensure health information is appropriately used or disclosed in an organization with multiple functions. |  |
| 3.1.0 – Administrative Safeguards  | 3.1.1 – Contingency Plans  | II. Policies and procedures must be implemented specifying how to respond to an emergency, or other unexpected occurrences (e.g., fires, natural disasters, system failures), that may damage systems containing health information.  |  |
| 3.1.0 – Administrative Safeguards  | 3.1.2 – Incident Procedures  | II. As part of an overall security program, policies and procedures must be implemented that describe how workforce members are to identify, report, respond, and mitigate security incidents affecting health information, as well as support the implementation of the incident response plan. |  |
| 3.1.0 – Administrative Safeguards  | 3.1.3 – Information Access Management  | II. Information access management policies and procedures must be developed, implemented and maintained, that specify who (persons or software programs) has access to what specific health information and under what conditions. |  |
| 3.1.0 – Administrative Safeguards | 3.1.4 – Security Management Process | II. Health information must be protected through implementation of security policies and procedures that address all of the following:* Periodic risk analyses (every two [2] years)
* Implementation of risk management activities
* A workforce member sanction policy
* Regular review of information system activity (such as review of audit logs and incident tracking reports)
* Documentation of measures
 |  |
| 3.1.0 – Administrative Safeguards | 3.1.7 – Verification of Identity | II. Policies and procedures must be implemented and maintained which specify that prior to disclosing health information, the identity of the requestor must be verified, and the authority that entitles the requestor to access health information must be established. |  |
| 3.2.0 – Physical Safeguards | 3.2.2 – Device and Media Controls | II. Policies and procedures must be implemented to govern the receipt, re-use, and removal of devices and media that contain health information, into and out of an entity/organization, and the movement of these items within the entity/organization. |  |
| 3.2.0 – Physical Safeguards | 3.2.3 – Facility Access Controls | II. Policies and procedures must be implemented to limit physical access to a state entities electronic information systems, used to store and process health information, and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |  |
| 3.2.0 – Physical Safeguards | 3.2.4 – Workstation Use and Security | III. A. State entities are responsible to implement workstation and mobile device security policies and procedures to specify the proper functions to perform, the manner in which they are performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access health information. In addition, the policies and procedures should protect health information from unauthorized access. |  |
| 3.3.0 – Technical Safeguards | 3.3.1 – Audit Controls | III.A. State entities are responsible to develop and [implement](#ImplementationDef) policies and procedures for regularly monitoring and reviewing audit records of their electronic information systems that contain, or use, electronic health information, to ensure that activity on those electronic systems is appropriate. |  |
| 3.3.0 – Technical Safeguards | 3.3.2 – Encryption | III. A. State entities are responsible for implementing policies and procedures regarding the encryption methods their organization utilizes to prevent unauthorized access to health information. |  |
| 3.3.0 – Technical Safeguards | 3.3.4 – Integrity | III. A. State entities are responsible to implement policies and procedures that safeguard, and maintain the integrity of, health information from being improperly altered or destroyed during processing, in storage, or while in transit. |  |
| 3.3.0 – Technical Safeguards | 3.3.5 – Access Control | III.A. For all information systems that contain health information, policies and procedures must be implemented that limit access only to those persons or software programs that have been granted access rights according to applicable state and federal requirements. |  |
| 3.4.0 – Policy and Procedures | 3.4.1 – Documentation | II. Security policies and procedures must be developed, implemented, utilized and maintained to ensure the confidentiality, integrity, and availability of health information that is created, received, maintained, and transmitted. |  |
| 4.1.0 – Administrative Requirements  | 4.1.1 – Policies and Procedures  | III. A. State entities are responsible to develop and maintain operational privacy policies and procedures that are compliant with SHIPM. |  |
| 4.1.0 – Administrative Requirements | 4.1.3 – Sanctions for Violation  | II. Policies and procedures must specify appropriate sanctions outlining what the consequences will be against any workforce member who improperly views, uses, or discloses health information. |  |
| 4.6.0 – Requirements for Specific Organizations | 4.6.5 – Hybrid Entities | II. Policies and procedures must be implemented and maintained which outline the requirement for Hybrid Entries to create and maintain adequate “firewalls” or separation between covered and non-covered healthcare components within their organization. |  |
| 5.1.0 – Accounting of Disclosures | 5.1.1 – Accounting of Disclosures | III. A. State entities are responsible to create, implement, and maintain policies and procedures stating how to process and document disclosures of health information as well as patient requests for an accounting of disclosure. |  |
| 5.2.0 – Amendments | 5.2.1 – Patient’s (Individual’s) Right to Amend Medical Records | III. A. State entities are responsible to create, implement, and maintain policies and procedures stating how to process and document patient requests for amendment to their medical records. |  |
| 5.4.0 – Patient Rights - Access | 5.4.1 – Patient’s (Individual’s) Right to Access Health Information | III. F. 1. State entities are responsible to implement policies and procedures. |  |

1. Note – this column provides the SHIPM policy reference (either II. Policy or III. Implementation Specifics) along with the policy requirement [↑](#footnote-ref-1)