The following provides a checklist 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.

| **SHIPM Section** | **SHIPM Policy** | **SHIPM Policy Reference Requirement[[1]](#footnote-1)** | **Completed?** |
| --- | --- | --- | --- |
| 2.1.0 – Authorizations | 2.1.1 – Authorizations | II. Policies and procedures must be implemented and maintained which outline requirements for when a patient authorization is needed and what must be included. |  |
| 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. |  |
| 2.2.8 – Opportunity to Agree or Object | II. Policies and procedures must be implemented and maintained to allow patients the opportunity to agree or object to specific uses and disclosures of their health information. |  |
| 2.2.15 - Underwriting | III. E. 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. |  |
| 2.2.18 – 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. |  |
| 2.3.0 – Specially Protected Information | 2.3.2 – HIV/AIDS Information | III. A.  3. Develop and implement policies and procedures regarding the collection, use and/or disclosure of public health records containing HIV/AIDS information.  4. Develop and implement policies and procedures regarding the disclosure of HIV/AIDS test results. |  |
| 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. |  |
| 2.4.0 Breach and Breach Notification | 2.4.1 – Breach and Breach Notification | III. B. Policies and procedures must be implemented and maintained to ensure compliance with legal requirements regarding investigating and reporting breaches or unauthorized disclosures of unencrypted or unsecured 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.  (see also sub items 1-3) |  |
| 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. |  |
| 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. (see also III. A for specifics) |  |
| 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. (see also III for more specifics) |  |
| 3.1.3 – Information Access Management | II. Information access management policies and procedures must be developed, implemented and maintained, that specify who has access to what specific health information and under what conditions. (see also III for more specifics) |  |
| 3.1.4 – Risk Analysis | II. Health information must be protected through implementation of security policies and procedures…(see also III for more specifics) |  |
| 3.1.7 – Verification of Identity | II. Policies and procedures must be implemented and maintained (i.e., periodically updated, on file, and used regularly) 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. |  |
| 3.1.8 – Workforce Security | II. (and III. A.) State entities are responsible to implement policies and procedures that limit or restrict access of health information to only those workforce members whose work requires access. |  |
| 3.2.0 – Physical Safeguards | 3.2.1 – Access Control | II. Information access management policies and procedures must be developed, implemented and maintained, that specify who has access to what specific health information and under what conditions. (see also III. A for more specifics) |  |
| 3.2.2 – Device and Media Controls | II. Policies and procedures must be implemented to govern the receipt and removal of hardware and electronic media that contain health information, into and out of an entity/organization, and the movement of these items within the entity/organization. |  |
| 3.2.3 – Facility Access Controls | II. Procedures must be implemented to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. |  |
| 3.2.4 – Workstation Use and Security | III. State entities are responsible for implementing workstation and mobile device security policies and procedures to ensure health information is protected from unauthorized access. In addition, the policies and procedures should specify the proper functions to be performed, 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. (see also III. for specifics) |  |
| 3.3.0 – Technical Safeguards | 3.3.1 – Audit Controls | II. Implement hardware, software, and policies and procedures to record and examine activity accessing health information in electronic information systems. |  |
| 3.3.2 – Encryption | II. and 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. |  |
| 3.3.3 – Access Administration | II. Technical policies and procedures must be developed, implemented, and maintained for electronic information systems that utilize electronic health information, to allow access only to those persons or software programs that have been granted access rights.  (see also III for more specifics) |  |
| 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, or transmitted.  (see also III for more specifics) |  |
| 4.1.0 – Administrative Requirements | 4.1.1 – Policies and Procedures | This item provides overall policy for development and maintenance of policy and procedure documentation. |  |
| 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. |  |
| 5.2.0 – Amendments | 5.2.1 – Patient’s (Individual’s) Right to Amend Medical Records | III. A. State entities are responsible to create 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. D. 1 and 4 State entities are responsible to implement policies and procedures…  (see item for more specifics) |  |
| 5.5.0 – Restriction for Self-Pay and Confidential Communication | 5.5.1 – Restriction for Self-Pay and Confidential Communication | III. B. 3 State entities are responsible to develop a process to ensure the appropriate patient address and/or phone number is recorded in the system or medical record and is used when communicating with the patient. |  |

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