|  |
| --- |
| **TITLE: Security Management Policy**  |
| **DEPARTMENT: Information Technology, Human Resources, Operations** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
| **05/31/22** |  |  |
| **Prepared by: Donny Friday, Dir. Of Technology** | **Date: 5/31/22** |
| **Administrative Approval:** Chief Executive Officer, Chief Information Officer, and Compliance Officer |
| CEO: Joe LaRue | Date: 05/31/22 |
| CIO: Tony Yi | Date: 05/31/22 |
| CO: Sharon Grambow | Date: 05/31/22 |
| **All other related polices/procedures/protocols:**  |

SEE LAST PAGE FOR REVIEW HISTORY

**Purpose:**

To establish a process to assess and manage security risks to information assets including ePHI.

**Scope and Applicability**

This policy applies to all Information Systems.

**Policy Statement**

A formal Security Management process shall be developed to assess, analyze, monitor, manage, remediate, and control risks to the Confidentiality, Integrity, and Availability of Information Systems and information assets.

**Procedures**

**General**

1. An inventory of Sun Health Information Systems that store, process, transmit, or receive ePHI and other Sensitive information will be developed and maintained.
2. Sun Health Information Systems that contain or impact ePHI or other Sensitive information will be classified based on their confidentiality, integrity, and availability requirements.

**Security Officer**

1. A Security Officer who is responsible for the development and implementation of security policies and procedures shall be identified.
2. The designated Security Officer should be a senior manager.
3. The Security Officer is responsible for overseeing the security management process including:
	1. Risk assessments and analysis;
	2. Security plans;
	3. Monitoring of security controls.
4. The Security Officer should provide regular updates to executive leadership.
5. The specific duties and responsibilities of the HIPAA Security Officer are defined in the Security Guidelines document.

**Policy and Procedures**

1. Reasonable and appropriate policies and procedures shall be implemented to comply with standards, implementation specifications, or other requirements of applicable regulations.
2. The Sun Health HIPAA Security Officer should perform tests of the internal controls of policies and procedures for adequacy and completeness.
3. A process shall be established for the review, approval, and distribution of policies and procedures.

**Risk Assessment**

1. An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information shall be conducted.
2. Risk assessments should be conducted for Information Systems that may have an impact on the confidentiality, integrity, and availability of ePHI or other Sensitive information.
3. Risk assessments should be conducted under the supervision of the HIPAA Security Officer.
4. Risk assessments should be conducted at least annually and after any significant changes to Information Systems.
5. The assessment should identify potential threats and vulnerabilities.
6. The assessment should evaluate the effectiveness of existing security controls and safeguards.
7. Threats should be evaluated based on likelihood that a vulnerability could be exploited.
8. The impact on confidentiality, integrity, or availability of ePHI and Information Systems that could result if a threat source successfully exploited a vulnerability should be evaluated.
9. Risks shall be determined based on the likelihood that threats will attempt to exploit vulnerabilities, the potential impact, and the effectiveness of security controls.
10. The assessment shall identify and prioritize corrective actions needed to mitigate risks.

**Risk Management**

1. Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be implemented.
2. Identified risks shall be prioritized based on the potential impact to ePHI and other Sensitive information, and resources shall be allocated accordingly.
3. Security methods to minimize or eliminate risks shall be identified based on their nature, feasibility, and effectiveness.
4. A cost-benefit analysis shall be considered in determining the extent of implementation of identified security methods.
5. Selected security methods shall be implemented under the direction of the Sun Health HIPAA Security Officer.
6. Implemented security methods shall be evaluated and revised as necessary by the HIPAA Security Officer.

**Security Planning**

1. The Security Officer shall develop and implement an effective risk management program to regularly monitor and evaluate threats and risks to information systems.
2. A formal security plan shall be developed and maintained to track identified security risks and document remediation efforts.
3. Security related activity shall be planned and communicated as appropriate to minimize the impact on the organization.
4. The Security Officer shall meet regularly with Information Systems and security related staff members and incorporate security measures into daily activities.

**Evaluation**

1. A periodic technical and nontechnical evaluation, based upon the standards implemented, and in response to environmental or operational changes affecting the security of ePHI, shall be conducted.
2. The Security Officer should evaluate, on an ongoing basis, the effectiveness of security policies and procedures.
3. The Security Officer should immediately evaluate the impact of the following events and take appropriate actions to address security threats:
	1. Changes in the HIPAA Security or Privacy regulations;
	2. New federal, state, or local laws and regulations affecting PHI;
	3. Changes in technology, environmental, or business processes that may affect the security of Information Systems;
	4. A serious security violation, breach, or other security incident.

**Documentation**

1. A written, or electronic, record must be maintained of the policies and procedures and actions, activities, or assessments required to be documented, for compliance with regulations.
2. Required documentation must be retained for at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.
3. Documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains.
4. Documentation must be reviewed periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

**Review and Revision**

1. The Security Management program shall be reviewed, and revised if needed, on an annual basis.

**Enforcement & Exception Handling**

Failure to comply with this policy, associated procedures and guidelines may result in disciplinary actions up to and including termination of employment or termination of contracts. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to this policy must be submitted in writing. Prior to official approval of any exception, this policy must continue to be observed.

**Definitions**

**ePHI** - Protected Health Information that is stored in electronic format.

**Information System** –Meansany combination of information technology and people's activities that support Sun Health operational, management and decision making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

**Workforce Member** -Means employees and other persons whose conduct, in the performance of work, are under the direct control of Sun Health, whether or not they are paid by Sun Health. This includes full and part time employees, contractors, affiliates, associates, students, and volunteers.

**Breach** - An impermissible use or disclosure under HIPAA that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

**Security Incident** - The attempted or successful unauthorized access, use, modification, destruction, or interference with Information Systems.

**Distribution**

This policy should be distributed to applicable Workforce Members. Recipients of this policy must acknowledge their receipt and understanding of this policy by referring any questions or problems with the policy within ten days of the issue date to the HIPAA Security Officer. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

**Applicable Regulations**

|  |  |
| --- | --- |
| **HIPAA Security Rule** | **45 CFR Part 160 and Subparts A and C of Part 164** |
| Security Management Process  | §164.308(a)(1),  |
| Risk Analysis | §164.308(a)(1)(ii)(A) |
| Risk Management | §164.308(a)(1)(ii)(B) |
| Assigned Security Responsibility  | §164.308(a)(2) |
| Evaluation | §164.308(a)(8) |
| Policies and Procedures | §164.316(a) |
| Documentation Maintenance | §164.316(b)  |
| Time Limit | §164.316(b)(1)(i) |
| Availability | §164.316(b)(2)(i) |
| Updates | §164.316(b)(1) |

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date: | Reviewed/Revised by: | New Changes | No Change | Revision(s): State reason for revision | INITIALS |
| √ one |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This policy is subject to the Master Service Agreement, confidential, and for internal business use only.

Nothing contained herein shall be construed as conferring by implication, estoppel or otherwise any license or other grant of right to use this customized intellectual property of BOC, except as expressly provided herein. This intellectual property was created for clients of blue orange compliance (BOC) for their sole and exclusive use. This property is not intended for the resale or reuse, except as BOC may voluntarily choose to transfer such property, in full, or in part. All customized work has a lifespan where it remains applicable for a client. BOC is not responsible for misprints, out-of-date information, technical inaccuracies, typographical or other errors appearing in this intellectual property. All information and related materials it contains are provided "AS IS", and is not intended to be legal advice. BOC makes no representation or warranty whatsoever regarding the completeness, accuracy, currency, or adequacy of, or the suitability, functionality, or availability, of the information or materials it contains. By ongoing use of this material without the availability of a current support contract from BOC, client assumes the risk that the information and materials may no longer be complete, accurate, in date, or may not meet your needs and requirements.