|  |
| --- |
| **TITLE: Workforce Security Policy**  |
| **DEPARTMENT: Information Technology, Human Resources, Operations** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday** | **Date: 05/31/21** |
| **Administrative Approval:** Chief Executive Officer, Chief Information Officer, and Compliance Officer |
| CEO: Joe LaRue | Date:  |
| CIO: Chip Burns | Date:  |
| CO: Sharon Grambow | Date:  |
| **All other related polices/procedures/protocols:**  |

SEE LAST PAGE FOR REVIEW HISTORY

**Purpose:**

To establish procedures ensuring that security requirements are incorporated as a part of the personnel hiring, transfer, disciplinary, termination, and supervision procedures.

**Scope and Applicability**

This policy applies to Workforce Members.

**Policy Statement**

Policies and procedures must be implemented to ensure that Sun Health, and all members of its workforce have appropriate access to ePHI and to prevent those Workforce Members who do not have access from obtaining access to ePHI.

**Procedures**

**General**

1. Any Sun Health Workforce Member who retains, accesses, or discloses ePHI data for unauthorized usage will be subject to disciplinary actions.
2. Alleged, apparent, or potential violations of policies and procedures must be reported as soon as possible, and no more than twenty-four (24) hours after violation becomes known, to a supervisor, Human Resources, Director of Business Applications, Director of Technolopgy, CIO or a HIPAA Officer.
3. Upon receiving a report of a possible violation, a confidential investigation of the alleged violation must be conducted.

**Workforce Screening**

1. Background checks will be conducted on potential Workforce Members during the hiring process:
	1. Background checks will verify references, academic qualifications, work experience, criminal history, and any state or federal healthcare sanctions;
	2. The type and number of background checks will depend on specific job function and level of access to ePHI as outlined in the job description;
	3. Only authorized personnel may conduct screening procedures and will protect the confidentiality of background verification checks.
2. Sun Health Workforce Members may be granted access to Information Systems only after meeting necessary background verification check requirements.
3. A separate background verification process will be conducted for existing Workforce Members who may be assigned a new job function that requires ePHI access.

**Confidentiality and Security**

1. All Sun Health Workforce Members shall be required to sign agreements upon hire or reassignment from previous position to:
	1. Protect the confidentiality of ePHI and other Sensitive information;
	2. To use Information Systems in an authorized manner;
	3. To read, understand, and adhere to policies and procedures.

**Job Categorization**

1. Procedures shall be implemented to determine that the access of a workforce member to ePHI is appropriate.
2. Specific job duties and responsibilities, including authorized levels of ePHI access necessary and associated risk levels, should be defined.
3. Authorization to access ePHI and other Sensitive information should be granted based on defined job duties.

**Authorization and Supervision**

1. Procedures shall be implemented for the authorization and/or supervision of Workforce Members who work with ePHI or in locations where it might be accessed.
2. All requests for granting, modification, or termination of access to ePHI and other Sensitive information must be submitted in writing and approved by an authorized manager or supervisor.
3. Appropriate corrective actions shall be taken for Workforce Members who have access to ePHI beyond the minimum necessary for the job function or duties.

**Job Changes**

1. Changes in access levels for Workforce Members granted access to ePHI and other Sensitive information shall be authorized and documented by either the Director of Business Systems or Director of Technology.
2. The Workforce Member’s access to ePHI within their current role must be terminated as of the date of transfer.
3. Using the appropriate CAR form, the Sun Health Workforce Member’s new manager or supervisor shall be responsible for requesting access to ePHI commensurate with the Workforce Member’s new role and responsibilities including:
	1. Date and time of modification;
	2. Identification of Workforce Members whose access is being modified;
	3. Description of modified access rights;
	4. Reason for modification of access rights.

**Termination Procedures**

1. Procedures shall be implemented for terminating access to ePHI and other Sensitive information when the employment of a Workforce Member ends or when access is no longer appropriate to the Workforce Member’s role or responsibility.
2. Timely notification must be provided to Information Services and other affected departments when a Workforce Member’s access to ePHI or other Sensitive information has been terminated.
3. Procedures shall be established to ensure that when a Workforce Member or User’s employment is terminated:
	1. All of the Workforce Member’s accounts with access to ePHI are disabled;
	2. Access to other Information Systems are disabled;
	3. The Workforce Member’s access to all facilities housing ePHI is terminated;
	4. Codes or passwords for systems, equipment access passwords (routers, switches, etc.), administrator passwords, and other common access control information shall be changed, as appropriate;
	5. Any equipment or property such as ID badges, personal computers, physical keys, flash drives etc. provided to the Workforce Member is returned to the organization.
4. A record of the termination of access shall be maintained including:
	1. The date and time notice was issued;
	2. The expected date of separation;
	3. A detailed record of the steps taken to terminate access.
5. Access to ePHI shall not be extended to any Workforce Member beyond the date of termination unless one of the following conditions have been met:
	1. A Business Associates Arrangement is entered into with the Workforce Member;
	2. The Workforce Member will be accessing ePHI as part of a specifically authorized arrangement with valid HIPAA consent documentation.

**Disciplinary Actions**

1. Appropriate sanctions shall be applied against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
2. Procedures for appropriate sanctions shall be established for circumstances where it has been determined that HIPAA or organizational policies and/or procedures have been violated.
	1. Sanctions can include, but are not limited to:
		1. Termination of employment;
		2. Civil penalties as provided under HIPAA or other applicable federal, state, or local laws;
		3. Criminal penalties as provided under HIPAA or other applicable federal, state, or local laws.

**Third Parties**

1. Business associates may be permitted to create, receive, maintain, or transmit ePHI on our behalf only if we have obtained satisfactory assurances that the business associate will appropriately safeguard the information.
2. Third parties shall be required to sign appropriate agreements to protect the confidentiality, availability, and integrity of ePHI and other Sensitive information prior to being granted access to Information Systems.
3. Business associate contracts and other arrangements must conform to the applicable standards and specifications of the HIPAA Security Rule.
4. Procedures shall be established to remove or modify access in a timely manner for third party personnel who have been terminated or no longer require access to ePHI or other Sensitive Information.

**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](http://en.wikipedia.org/wiki/Information_technology) and people's activities that support operational, management and decision making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

**Workforce Member** –Means Sun Health employees and other persons whose conduct, in the performance of their work, is 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, volunteers, and staff from third party entities who provide services.

**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** |
| Sanction Policy | §164.308(a)(1)(ii)(C) |
| Workforce Security | §164.308(a)(3)(i) |
| Authorization and/or Supervision | §164.308(a)(3)(ii)(A) |
| Workforce Clearance | §164.308(a)(3)(ii)(B) |
| Termination Procedures  | §164.308(a)(3)(ii)(C) |
| Business Associate Contracts and Other Arrangements | §164.308(b)(1), §164.308(b)(4), §164.314(a)(1), §164.314(a)(2)(i), §164.314(a)(2)(ii) (A), §164.314(a)(2)(ii)(B) |

**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.