|  |
| --- |
| **TITLE: Physical and Environmental Security Policy**  |
| **DEPARTMENT: Information Technology, Human Resources, Operations** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Dir. Of Technology** | **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 implement security measures to restrict access to facilities and Sun Health Information Systems from unauthorized physical access, tampering, theft, and physical damage, while ensuring that access by authorized workforce members is allowed.

**Scope and Applicability**

This policy applies to all facilities, locations and Sun Health Information Systems.

**Policy Statement**

Appropriate measures shall be taken to protect facilities and Information Systems from unauthorized physical access, tampering, theft, and physical damage, while ensuring that access by authorized workforce members is allowed.

**Procedures**

**General**

1. Security measures may be employed including security personnel, electronic controls, and video monitoring to deter unauthorized entry.
2. Distribution of keys or electronic access codes, prox cards, etc., shall be provided to authorized personnel only.
3. Procedures shall be developed and maintained to record the distribution and revocation of keys and access rights.
4. Any incident involving the misplacement or theft of a master facility key must be reported to the Security Officer.
5. Physical locks and/or electronic access codes shall be changed as appropriate based on risks to unauthorized physical access.
6. Workforce members must be vigilant of non-authorized personnel present in their work areas and report any incidents as warranted.
7. Repairs and modifications related to the physical security of facilities that house PHI must be conducted by authorized personnel and documented as appropriate.

**Information System Components**

1. Information Systems shall be placed in locations to minimize the risk of physical damage.
2. Access to data centers that store or process ePHI will be locked and restricted to authorized persons only.
3. Primary and backup data centers shall be physically located to minimize the possibility of damage to both facilities during a disaster and to maximize their availability for recovery efforts.
4. Doors to Sun Health network wiring/communications closets will be locked and restricted to authorized persons only.
5. Information Systems, including workstations and laptops, located in non-secure work spaces shall employ additional physical safeguards as appropriate.
6. Logs shall be maintained to track access by visitors or vendors that perform work to, or in, facilities that store or process ePHI.

**Physical Access for Workforce Members**

1. Access rights to sensitive areas shall be provided only as needed to accomplish job duties. Roles that require access rights to sensitive areas shall be defined and documented.
2. Access rights for facilities that house ePHI systems shall be periodically reviewed and revised as necessary.
3. Physical access to facilities that house ePHI systems shall be tracked, recorded, and maintained in a secure manner.
4. Workforce members shall not attempt to gain physical access to facilities for which they do not have proper authorization.
5. Workforce members shall immediately report the loss or theft of any keys that grant them physical access to facilities.
6. Workforce members shall carry an identification badge when at facilities that house ePHI systems.
7. Workforce members who observe a person attempting to bypass any security measure shall report that person to security personnel or the Security Officer.

**Contingency Operations**

1. In the event of a disaster or other emergency, physical access to Sun Health facilities that house ePHI systems shall be controlled and access granted only to workforce members authorized in contingency and emergency plans.

**Review and Revision**

1. Physical Security controls and procedures shall be periodically reviewed for appropriateness and effectiveness.

**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.

**PHI** – Protected Health Information. Means all individually identifiable health information held or transmitted by Sun Health, a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral.

**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.

**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** |
| Facility Access Controls | §45 CFR 164.310(a)(1) |
| Contingency Operations | §45 CFR 164.310(a)(2)(i) |
| Facility Security Plan | §45 CFR 164.310(a)(2)(ii) |
| Access Control and Validation Procedures | §45 CFR 164.310(a)(2)(iii) |
| Maintenance Records | §45 CFR 164.310(a)(2)(iv) |
| Security Management Process  | §164.308(a)(1), §164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B) |
| Contingency Plan  | §164.308(a)(7)(ii)(E) |

**Revision History**

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

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.