|  |
| --- |
| **TITLE: Media Protection Policy**  |
| **DEPARTMENT: Information Technology** |
| **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 define and document appropriate procedures and controls to protect the confidentiality and integrity of Sensitive information stored on Digital Media.

**Scope and Applicability**

This policy applies to all Sun Health Workforce Members and all Digital Media containing Sensitive information.

**Policy Statement**

Appropriate procedures and controls shall be established and implemented to prevent unauthorized access to Sun Health Sensitive information stored on Digital Media. Media Protection controls and procedures shall be regularly reviewed for appropriateness and effectiveness.

**Procedures**

**Digital Media**

1. Only authorized Workforce Members are permitted to access Digital Media.
2. Digital Media must be managed and tracked throughout its lifecycle including acquisition, movement, and destruction.
3. Portable Digital Media, including USB storage and external hard drives, must be approved and sanitized prior to first use.
4. Portable Digital Media containing Sensitive information must be encrypted using appropriate standards.
5. Portable Digital Media containing Sensitive information shall be identified with appropriate markings if feasible.

**Backup Media**

1. Backup media containing protected health information (PHI), personally identifiable information (PII), or other Sensitive information shall be encrypted.
2. Backup media must be stored in a secure off-site location protected by a locking mechanism only accessible by authorized personnel.
3. Personnel must be specifically authorized by Sun Health to access to the secure storage area and records of that access must be maintained.
4. Visitors to the secure storage area must be escorted at all times. A visitor log shall be maintained to document escorted visitor access.
5. Backup media shall be retired before its maximum usages or maximum age is reached.
6. Backup media that is reused, or no longer used or needed, must be destroyed in accordance with applicable media sanitation procedures.

**Media Transport**

1. Digital Media containing Sensitive information shall be protected and controlled during transport.
2. Only authorized personnel may transport Digital Media containing Sensitive information.
3. All activities surrounding the transport process shall be documented.

**Media Sanitation**

1. Digital Media shall be sanitized prior to disposal or re-use by utilizing industry accepted sanitization techniques.
2. Records shall be maintained that track and document sanitization and disposal actions.

**Review and Revision**

1. Media Protection 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**

**Digital Media** –Meansany physical electronic media used to store information in a machine readable format (ex. hard drives, random access memory, read only memory, tapes, CD’s, network equipment, solid state drives, etc.)

**Portable Digital Media –** Digital Media capable of storing information that can be used to transport information including external or removable hard drives, USB storage devices, CDs, DVDs and mobile computing devices capable of storing information including laptops, tablets, and smartphones.

**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** |
| Authorization and/or Supervision | §45 CFR 164.308(a)(3)(ii)(A) |
| Workstation Security | §45 CFR 164.310(c) |
| Device and Media Controls | §45 CFR 164.310(d)(1) |
| Disposal  | §45 CFR 164.310(d)(2)(i) |
| Media Re-Use | §45 CFR 164.310(d)(2)(ii) |
| Accountability | §45 CFR 164.310(d)(2)(iii) |
| Data backup and Storage | §45 CFR 164.310(d)(2)(iv) |
| Integrity | §45 CFR 164.312(c)(1) |
| 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.