|  |  |  |
| --- | --- | --- |
| **TITLE: User ID and Password Policy** | | |
| **DEPARTMENT:** | | |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by:** | | **Date:** |
| **Administrative Approval:** Chief Executive Officer, Chief Information Officer, and Compliance Officer | | |
| CEO: | | Date: |
| CIO: | | Date: |
| CO: | | Date: |
| **All other related polices/procedures/protocols:** | | |

SEE LAST PAGE FOR REVIEW HISTORY



**Purpose:**

To create, maintain, and protect User ID’s, passwords, and authentication procedures.

**Scope and Applicability**

This policy applies to all Sun Health Information Systems containing or accessing ePHI or other Sensitive information.

**Policy Statement**

Sun Health Information Systems containing ePHI or other Sensitive information shall employ procedures and security controls that only permit Access to authorized Users once their identification has been verified and authenticated.

**Procedures**

**General**

1. Procedures and technical controls shall be implemented to verify that a person or entity seeking access to Sun Health Information Systems is the one claimed.
2. If any Sun Health Workforce Member believes that their user identification and/or password have been compromised, they must report the incident immediately to the Service Desk, Director of Technology or Director of Business Systems.
3. Sun Health Workforce Members are strictly prohibited to ask for, or use another person’s identification and/or password information.
4. Except when authorized by Information Technology, the reuse of User identifiers after a Sun Health Workforce Members’ Access to Information Systems has been terminated is prohibited.
5. Access to Information Systems may be tracked and monitored.

**User Identification**

1. Sun Health Information Systems shall uniquely identify and authenticate Users for Access to ePHI and other Sensitive information.
2. An exception may be granted for shared workstations, such as nursing stations, treatment rooms, etc. providing that:
   1. Access to applications containing ePHI require a unique User ID and Password.
   2. User ID’s and Passwords may only be shared as directed by Information Technology.
   3. Shared account passwords shall be changed periodically and at any other time warranted by security concerns.
3. Unique identifiers shall be assigned to Workforce Members to distinguish Users and track their activity.
4. Sun Health Workforce Members are responsible for ensuring that their assigned user identification is appropriately protected and only used for legitimate Access to networks, systems, or applications. Workforce Members may not share information pertaining to their user IDs, Passwords, personal identification numbers, etc.
5. Workforce Members must ensure that their User ID and Password are not documented, written, or otherwise exposed in an insecure manner.

**Passwords**

1. Procedures for creating, changing, and safeguarding strong Passwords shall be implemented and properly communicated.
2. Passwords must be used for authentication to all Sun Health Information Systems containing Sensitive information.
3. Passwords must be unique and not used for any other personal or non-work related purpose.
4. Passwords may not contain the User ID, person’s name, or any personal or identifying information.
5. Passwords must be hard to guess. Do not use whole words that can be found in a dictionary, proper names, or common phrases, substitutions or patterns.
6. Passwords must meet the length, complexity, life, and reuse requirements defined in the Information Security Guidelines document.
7. The Service Desk shall establish a process to reset Passwords upon request of a User. The process shall verify their identity and must be changed by the Workforce Member upon next login.
8. Passwords may not be e-mailed, texted or communicated insecurely.

**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.

**Access** -The ability or means necessary to read, write, modify, or communicate data/information or otherwise use Information Systems.

**Workforce Member** -Means 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.

**Users** -Are the individuals, groups, or organizations authorized to access information assets.

**Distribution**

This policy should be distributed to applicable Sun Health 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** |
| Password Management | §164.308(a)(5)(ii)(D) |
| Unique User Identification | §164.312(a)(2)(i) |
| Person or Entity Authentication | §164.312(d) |

**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.