|  |  |  |
| --- | --- | --- |
| **TITLE: Audit Policy** | | |
| **DEPARTMENT:** | | |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Director 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 create and conduct periodic reviews of audit trails of Information Systems activities.

**Scope and Applicability**

This policy applies to Information Systems containing or confidential, ePHI, financial, and other sensitive and private information.

**Policy Statement**

Reasonable and appropriate procedures shall be established and maintained to conduct periodic reviews of Information Systems activity.

**Procedures**

**General**

1. Procedures shall be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; all departments must work with the technology department to provide updated information on employment status or role changes that impacts access to information.
2. The type and frequency of auditing mechanisms to be implemented shall be based on the following factors:
   1. Confidentiality of the information;
   2. The importance of the Availability of the Information System;
   3. Connectivity with other systems and the resulting degree of risk;
   4. Findings from the audit process.
3. Proactive audits are to be performed periodically with the intent of sampling the data to identify possible inappropriate use or activity.
4. Incident based audits shall be performed when identified events trigger the need for an audit.

**Auditable Events**

1. Hardware, software, and/or procedural mechanisms should be implemented that record and examine activity in information systems that contain or use ePHI.
2. Audits should be established and conducted for system level events and for application level events.
3. Procedures should be implemented for monitoring log-in attempts and reporting discrepancies.
4. As appropriate, auditable events should include:
   1. Access or modification of ePHI and other Sensitive information;
   2. Successful and failed authentication attempts;
   3. Use of audit software programs or utilities;
   4. Information System start-up or shutdown;
   5. Use of privileged accounts, such as system administrators, superusers;
   6. Security incidents.

**Content of Audit Records**

1. When feasible, Information System activity auditing mechanisms should generate the following information:
   1. Date and time of activity;
   2. Description of attempted or completed activity;
   3. Identification of user performing activity;
   4. Origin of activity, such as IP address or workstation ID.
2. Audit logs should be configured to capture and retain sufficient history to meet regulatory requirements and security objectives.

**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 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 the 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** |
| Information System Activity Review | §164.308(a)(1)(ii)(D) |
| Log-in Monitoring | §164.308(a)(5)(ii)(C) |
| Audit Controls | §164.312(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.