A. Administrative Safeguards

45 CFR §164.308[1]

Administrative Safeguards are designed to be reasonable and appropriate in establishing the foundation for our security program. This includes the development, implementation and maintenance of security measures necessary to safeguard protected health information and to manage the conduct of our workforce in regard to the protection of that information.

1. Security Management Process

45 CFR §164.308(a)(1)

Procedures have been adopted to prevent, detect, contain, correct and document security violations.[2] ***The Risk Analysis and Risk Management*** processes form the foundation upon which security activities are built.[3] We hereby incorporate portions of NIST 800 Series of Special Publications (SP), specifically SP 800-30 Rev 1 *Guide for Conducting Risk Assessments*[4] to the extent they provide relevant guidance to our implementation activities. Particular attention is to be paid to the explanations of terms as used in NIST SP 800-30 including "vulnerability," "threat," and "risk," and the relationship among the three terms in understanding this policy as stated in the Committee on National Security Systems Instruction No. 4009 "National Information Assurance Glossary."[5]

(a) Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

(b) Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

---

[1] Office of Civil Rights Guidance on Administrative Safeguards
[2] 45 CFR §164.308(a)(1)(i)
[3] 68 Fed. Reg. 8346.
[4] NIST Guide for Conducting Risk Assessments
[5] National Information Assurance Glossary, CNSS Instruction No. 4009

(c) Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) The adverse impacts that would arise if the circumstance or event occurs; and

(ii) The likelihood of occurrence.

(d) Risk Analysis

45 CFR §164.308(a)(1)(ii)(A)[6]

Assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information as required by regulations are conducted on a routine basis. This is accomplished by identifying and documenting potential threats and vulnerabilities and assessing security measures to determine the likelihood of a threat occurrence. The policy is to:

- Determine the potential impact;
- Determine the level of risk; and;
- Identify security measures for implementation and finalization of the necessary documentation.

(e) Risk Management

45 CFR §164.308(a)(1)(ii)(B)[7]

Security measures have been implemented that are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.[8] It is our policy to evaluate and maintain security measures and documentation on an on-going basis.[9]

(f) Information System Activity Review

45 CFR §164.308(a)(1)

It is our practice to periodically review various indicators and records of information system activity such as audit logs, access reports, and

[6] Office of Civil Rights Guidance on Risk Analysis Requirements
[7] NIST Risk Management Guide for IT Systems
[8] 45 CFR §164.306(a), General Requirements of the Security Rule.
[9] 45 CFR §164.316(b)(1)(ii)

security incident reports with a goal to prevent, detect, contain, and correct security violations or threats to protected health information regardless of form/format, electronic or otherwise. Such periodic reviews shall occur at intervals that are no longer than six months.

Information system activity reviews are documented.

(g) **Workforce Clearance** (*addressable)*

45 CFR §164.308(a)(1)(ii)(B)(ii)

(i) **Access Authorization**

Access authorization and/or supervision will be provided for workforce members who have access to electronic protected health information.

(ii) **Termination Procedure**

Access to all systems and facilities will be terminated when a member of the workforce or vendor Business Associate or no longer requires access to information or facilities in order to perform their assigned job.

2. Security and Privacy Officer(s)

45 CFR §164.308(a)(2)

Responsibility for the security of protected health information is designated to a Security and Privacy Committee including designated Security and Privacy Officer(s).

We have in place a process for receiving, documenting, tracking, investigating, and taking action on complaints concerning the organization's security and privacy policies. We maintain an accounting of (1) individuals who have access to protected health information maintained by each of our facilities and (2) uses and disclosures of confidential information as required by law.

3. Information Access Management Policy

45 CFR §164.308(a)(4)

Policies and procedures for granting access to sensitive information have been established.

- Members of the workforce will be routinely trained on appropriate access methods and on information access controls;

- Safeguards will be used as appropriate to control access to sensitive information;

- Members of the workforce are responsible for limiting their use of the type and amount of sensitive information necessary to carry out their assigned job role or function.

4. Security Awareness And Training Policy

45 CFR §164.308(a)(5) (*addressable)*

Workforce members will be trained in security policies and procedures on a routine basis, including the following:

- How to identify, report, and prevent potential security incidents;

- Procedures for guarding against, detecting, and reporting malicious software as needed to support anti-virus software utilized on all computers that connect to the internet and/or are networked together;

- Security reminders and periodic updates on security concerns;

- Log-in monitoring to identify log-in attempts and for reporting of discrepancies;

- Password management including education on procedures for creating, changing, and safeguarding passwords.

Security training will be an ongoing activity with periodic security reminders to keep workforce members up-to-date on potential threats at the discretion of the Security Officer.

5. Security Incident Procedures

45 CFR §§164.308(a)(6); 164.400; 164.402; 164.404; 164.406; 164.408; 164.410; 164.412; 164.414

It is the responsibility of the Security and Privacy Committee to identify and respond to security incidents. Responses to security incidents include, by way of example:

- Rapid identification and classification of the severity of security incidents;

- Determination of the risk to protected health information and the subject(s) thereof;

- Repairing or correcting the condition that created the security incident;
- Retrieving or limiting the dissemination of protected health information;
- Making a determination as whether the security incident rises to the level of a reportable breach under the HIPAA/HITECH regulations;
- Making a report of a breach, if required, to the appropriate parties;
- Mitigating any harmful effects of the security incident;
- Documenting security incidents, along with their causes and our responses.

We will continue to work towards expanding management and workforce members knowledge of security incident prevention through research, analyses of security incidents, and improved training and awareness programs for employees.

6. Contingency Planning & Emergency Access Operation Plan

45 CFR §164.308 (a)(7)(i)[10]

It is our policy to be prepared to safeguard protected health information during emergencies and contingency operations. The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency. This plan will include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures. [11]

(a) Contingency Planning Objectives

- An evaluation of the capability to restore operations at an alternate site (if necessary);
- An evaluation of the capability to recover operations using alternate equipment (if necessary);
- An evaluation of the capability to perform some or all of the affected business processes using other means;

[10] NIST High Impact System Template

[11] In the Final Rule, specifications. for testing and revision procedures, and an applications and data criticality analysis are *addressable*.

- An evaluation of the entire enterprise including all IT system components.

(b) National Institute of Standards and Technology (NIST) Guidance[12]

The organization, under the direction of the Security & Privacy Officer(s) will be guided by the recommendations of NIST in the area of contingency planning, following the seven key steps:

1. Develop the contingency policy objective statement;
2. Conduct a Business Impact Analysis (BIA);
3. Identify preventive controls;
4. Develop recovery strategies;
5. Create the contingency plan;
6. Conduct testing and training;
7. Review and maintain the plan.

(c) Plan Components

Contingency Plans to respond to emergencies including fire, vandalism, system failure, and natural disasters that damage electronic data systems are in effect. Oversight of the development, maintenance, and periodic testing of emergency plans is the responsibility of the designated Security and Privacy Committee. The components of the Plan include:

- Data backup process to create and maintain retrievable copies of electronic protected health information;
- Identification of crisis management team members who will address the strategic and tactical response of the organization in an emergency;
- Designation of a command center or designated facility to be utilized during emergency mode operation;
- Development of procedures and checklists to provide for the orderly transition and restoration of normal business operations;

[12] NIST Special Publication 800-34 Rev.1, Contingency Planning Guide

- Coordination and communication of the plan both internally and externally to business associates and others as appropriate while ensuring that health and safety issues are addressed.

7. Disaster Recovery Plan

45 CFR §164.308 (a)(7)(ii)(B)

The Disaster Recovery Plan (DRP) applies to major events, usually catastrophic, that deny access to normal operations for an extended period. This IT-focused plan is designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.

The Security Officer is responsible for the development of a Disaster Recovery Plan document. The Plan will include:

- Identification of the scope of the DRP (specific locations/sites and critical systems);
- Identification of a response team;
- Identification of a system of notifications (to alert necessary personnel of the incident);
- Compilation of a damage assessment and reporting process;
- Initiation of recovery operations for the return to normal operations.

Service agreements are maintained on software and hardware as necessary.

Recovery plans are tested and revised on a periodic basis, at least annually.