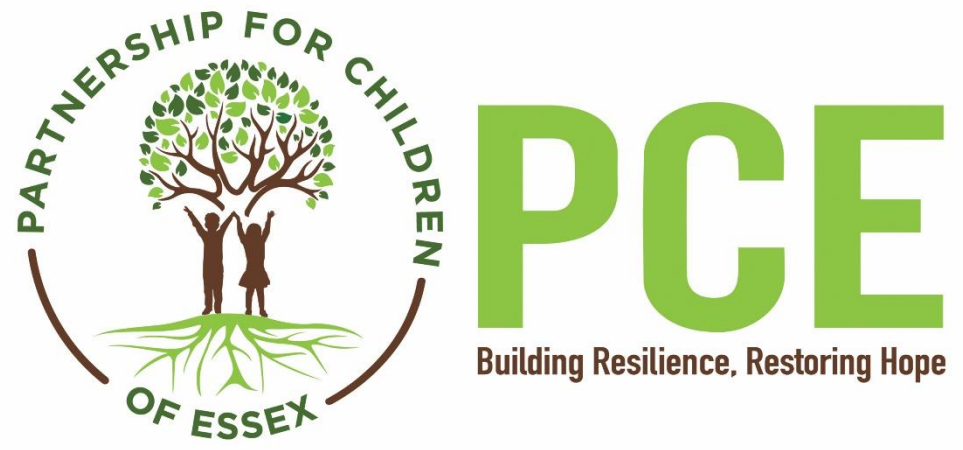

HIPAA SECURITY RULE POLICY MANUAL

HIPAA SECURITY RULE POLICY MANUAL

TABLE OF CONTENTS

PAGE

HIPAA SECURITY POLICIES:
HIPAA COMPLIANCE PROGRAM

Topic: **HIPAA COMPLIANCE – INTRODUCTION AND ADMINISTRATIVE MATTERS**

Date Adopted: May 1, 2020

Revised:

I. INTRODUCTION

This **HIPAA Security Rule Policy Manual** ("**Manual**") contains the HIPAA Security Rule Policies and Procedures of **Partnership for Children of Essex** (the "**Organization**"). This Manual, together with the Organization's HIPAA Privacy Rule Policy Manual, comprise the Organization's HIPAA Compliance Program.

The Organization's HIPAA Compliance Program manuals outline the steps that are being taken by the Organization to comply with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), as may be amended from time to time, including as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations (collectively, "HIPAA"). The manuals also address state laws and regulations governing the privacy and security of patient information.

Reflective of the Organization's commitment to conducting business in a lawful and ethical manner, this Manual has been approved by the Organization's Board of Trustees and constitutes official Organization policy. While the Organization recognizes that mistakes will occur, all workforce members have an affirmative, ethical duty to come forward and report violations or suspected violations of this Manual, as well as any patient complaint related to privacy and security, so that appropriate steps may be taken to address the issue. Workforce members who fail to comply with the policies and procedures set forth in this Manual will be subject to appropriate sanctions, including the possibility of termination. Further, compliance with these policies and procedures will be a factor in performance evaluations.

The Organization has designated a HIPAA Security Officer ("Security Officer") who oversees the implementation and oversight of the Security Rule Policy Manual and security program for the Organization, under the guidance and oversight of the Compliance Committee.

The Organization also has designated a HIPAA Privacy Officer ("Privacy Officer"), who oversees the Organization's HIPAA Privacy Rule Policy Manual and privacy program, and who coordinates efforts with the Security Officer. The Privacy Officer operates under the guidance and oversight of the Compliance Committee.

Questions concerning the policies and procedures set forth in this Manual should be directed to the Organization's Security Officer. The Security Officer will consult with the Privacy Officer, Compliance Committee and/or legal counsel where appropriate.

II. PROTECTED HEALTH INFORMATION; OTHER PROTECTED INFORMATION

Throughout this Manual, references are made to "Protected Health Information" or "PHI." Under HIPAA, this term is defined to mean any health information, including genetic information, transmitted or maintained in any form, that:

- Is created or received by a HIPAA covered entity;
- Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and
- Identifies the individual or offers a reasonable basis for identification.

PHI *does not include* individually identifiable health information (a) held by an organization strictly in its role as an employer, or (b) regarding a person who has been deceased for more than 50 years.

Federal privacy requirements for covered entities and their business associates are contained in the HIPAA Privacy Rule and HIPAA Security Rule. These rules require covered entities and their business associates to implement reasonable safeguards to protect PHI from uses and disclosures that are not permitted under HIPAA, including unauthorized access, alteration, deletion and transmission.

The HIPAA Privacy Rule governs <u>all</u> PHI, no matter what the form or format—whether oral, paper or electronic. The Organization's HIPAA Privacy Rule Policy Manual contains the Organization's privacy policies under the Privacy Rule. In addition to HIPAA, certain state laws impose obligations on the Organization to protect certain private information from improper uses and disclosures. These state law obligations are addressed in the Privacy Rule Policy Manual and this Manual.

The HIPAA Security Rule governs <u>only</u> electronic PHI, or "e-PHI," which includes PHI that is (a) transmitted by electronic means, or (b) maintained in electronic media. The Organization's policies and procedures under the Security Rule are contained in this HIPAA Security Rule Policy Manual.

III. TRAINING

The Organization will train all members of its workforce on the policies and procedures that comprise the Organization's HIPAA Compliance Program as necessary and appropriate for the purpose of carrying out each workforce member's job functions. New workforce members will receive training within a reasonable period of time after joining the Organization, and all workforce members will receive periodic training. Training will be conducted by or under the direction of the Privacy Officer.

Training will include information on at least the following topics:

- Uses and disclosures of patient information
- Patient privacy rights
- Privacy breaches
- Sanctions for violations of the requirements set forth in the Organization's HIPAA Compliance Program and/or HIPAA.

Each workforce member will certify that he/she received training and understands the Organization's HIPAA Compliance Program and the requirements of HIPAA. A form for such purpose is contained in the Organization's HIPAA Privacy Rule Policy Manual.

IV. SANCTIONS

Any violation of the Organization's HIPAA Compliance Program by any workforce member may result in disciplinary action, up to and including termination of employment or engagement. Discipline will be dispensed promptly and consistently based upon the nature, severity, and frequency of the violation, and without regard to the seniority, rank or position of the individual in violation.

The Organization's HIPAA Sanction Policy is contained in this Manual, in the policy entitled "Sanction Policy."

V. MITIGATION

The Organization will, to the extent practicable, mitigate any harmful effect due to inappropriate use or disclosure of e-PHI by a workforce member or by a Business Associate (or will require the Business Associate to mitigate any such harmful effect).

VI. RETALIATORY ACTS

The Organization will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the good faith exercise of any right, participation in any process, or opposition to any unlawful act or practice, set forth in the Organization's HIPAA Compliance Program. Further, the Organization will not threaten, intimidate, coerce, harass, discriminate against or take any other retaliatory action against any individual or person for:

1. Filing a complaint under 45 C.F.R. § 160.306;

2. Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing under 45 C.F.R. Part 160;

Opposing any act or practice made unlawful under 45 C.F.R. Part 160, Subpart C, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of Subpart E of 45 C.F.R. Part 164.

VII. IMPLEMENTATION OF PROGRAM; CHANGES TO POLICIES AND PROCEDURES

This Manual is intended to provide the Organization with information to assist the Organization with meeting the HIPAA Security Rule requirements. In order to ensure the Organization has incorporated all necessary elements of the Security Rule into its security program, the Organization will periodically perform risk and gap assessment of its risks and vulnerabilities and its administrative, physical and technical safeguards as required under the Security Rule. Information about risk assessments is contained in **Exhibit B** to this Manual.

In addition, the Organization will promptly change the policies and procedures set forth in the Organization's HIPAA Compliance Program as necessary and appropriate to comply with changes in applicable laws or regulations.

VIII. DOCUMENTATION

The Organization will maintain a written or electronic record of all written communications and any action, activity, or designation required to be documented as set forth in this Manual or related to the policies and procedures set forth herein. The Organization will retain the documentation in accordance with the applicable laws and regulations regarding the maintenance of such records, or six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

IX. REFERENCES

45 C.F.R. § 160.103 (definitions); 45 C.F.R. § 164.530(a)(1) (personnel designations); 45 C.F.R. § 164.530(b)(1) (training); 45 C.F.R. § 164.530(e)(1) (sanctions); 45 C.F.R. § 164.530(f) (mitigation); 45 C.F.R. § 164.530(g) and 45 C.F.R. § 160.316 (retaliatory acts); 45 C.F.R. § 164.530(i)(ii) (changes to policies and procedures); 45 C.F.R. § 164.530(j) (documentation).

HIPAA SECURITY POLICIES:
HIPAA COMPLIANCE PROGRAM

Topic: **OVERVIEW OF HIPAA SECURITY RULE**

Date Adopted: May 1, 2020

Revised:

I. COVERED ENTITIES AND BUSINESS ASSOCIATES

The HIPAA Security Rule applies to the following entities, known as "covered entities":

- Health care providers – providers of medical or other health services who transmit any health information in electronic form in connection with a transaction for which a standard has been adopted.
    - Covered transactions include the electronic transmission of: (1) health care claims or equivalent encounter information; (2) health care payment and remittance advice; (3) coordination of benefits; (4) health care claim status; (5) enrollment and disenrollment in a health plan; (6) eligibility for a health plan; (7) health plan premium payments; (8) referral certification and authorization; (9) first report of injury; (10) health claims attachments; and (11) other transactions that the government may prescribe by regulation.
- Health plans – individual or group plans that provide or pay the cost of health care.
- Health care clearinghouses – public or private entities that process health care transactions from a standard format to a nonstandard format, or vice-versa.

Any person or organization that qualifies as a "covered entity" under the HIPAA Privacy Rule is also required to comply with the HIPAA Security Rule. As a provider of care coordination that bills the New Jersey Medicaid program and other payors, the Organization is a HIPAA Covered Entity.

The 2013 HIPAA Omnibus Rule implemented a number of provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under HIPAA. Pursuant to the Omnibus Rule, "business associates" of covered entities, as well as "subcontractors" of business associates (collectively referred to in this Manual as "business associates"), must comply with the Security Rule requirements as they pertain to e-PHI the business associate creates, receives, maintains or transmits on behalf of a HIPAA covered entity.

Business Associate. The term "business associate," when used in this Manual, will have the same meaning as set forth in 45 C.F.R. § 160.103 and means, with respect to a covered

entity, a person or corporate entity that, on behalf of the covered entity (or on behalf of an organized health care arrangement in which the covered entity participates), *but other than in the capacity of a member of the workforce of the covered entity (or the organized health care arrangement)*:

- Creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA's Administrative Data Standards and Related Requirements subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.20, billing, benefit management, practice management, and repricing; or

- Provides legal, actuarial, accounting, consulting, data aggregation (as defined in 45 C.F.R. § 164.501), management, administrative, accreditation, or financial services to or for the Organization (or to or for an organized health care arrangement in which the Organization participates), where the provision of services involves the disclosure of PHI from the Organization (or organized health care arrangement in which the Organization participates), or from another business associate of the Organization (or organized health care arrangement in which the Organization participates), to the person or corporate entity.

A business associate *includes* a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

A business associate *does not include* a health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual. (***Note, however***, that a health care provider/covered entity may act as a business associate of another health care provider/covered entity if performing business associate functions as set forth above.)

Subcontractor. The term "subcontractor" means a person to whom a HIPAA business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

II. ELECTRONIC PROTECTED HEALTH INFORMATION ("e-PHI")

The Security Rule applies only to electronic protected health information ("e-PHI") created, received, maintained or transmitted by a HIPAA covered entity, or by a HIPAA business associate on behalf of a covered entity. E-PHI is protected health information (a) transmitted by electronic means, or (b) maintained in electronic media.

Electronic media includes electronic storage media on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Electronic media also includes transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including the transmission of paper, via facsimile, and of voice, via

telephone, are not considered transmissions via electronic media if the transmission being exchanged did not exist in electronic form immediately before the transmission.

III. GOALS OF THE HIPAA SECURITY RULE

The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of e-PHI.

- Confidentiality means the "data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity means the "data or information has not been altered or destroyed in an unauthorized manner."
- Availability means the "data or information is accessible and usable upon demand by an authorized person."

The Security Rule also requires HIPAA covered entities and business associates to protect against any reasonably anticipated improper disclosures of e-PHI, and any reasonably anticipated threats or hazards to the security or integrity of e-PHI. Furthermore, covered entities and business associates must ensure compliance with the Security Rule requirements by members of their workforce. The Security Rule does not require that covered entities and business associates guarantee *absolute* security, but that reasonable safeguards have been instituted to protect against reasonably anticipated threats or hazards.

IV. SECURITY STANDARDS

The Security Rule mandates that HIPAA covered entities and business associates meet a series of security standards. Each security standard can be categorized as being an administrative, physical, or technical safeguard. Every standard must be met.

- *Administrative Safeguards* are administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of a covered entity's workforce in relation to the protection of that information.
- *Physical Safeguards* are security measures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- *Technical Safeguards* are the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

V. IMPLEMENTATION SPECIFICATIONS

Implementation specifications provide instructions for implementing the Security Rule standards. Each implementation specification is either required or addressable.

- *Required implementation specifications.* If an implementation specification is required, the Organization must implement the specification.

- *Addressable implementation specifications.* If an implementation specification is addressable, the Organization must:

    - Assess whether the implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting e-PHI; and

    - As applicable to the Organization:

        - Implement the implementation specification if reasonable and appropriate; or

        - If implementing the implementation specification is not reasonable and appropriate:

            - Document why it would not be reasonable and appropriate to implement the implementation specification; and

            - Implement an equivalent alternative measure if reasonable and appropriate.

Thus, "addressable" does not mean the Organization can ignore the specification.

The Organization must review and modify the security measures implemented under the Security Rule as needed to continue provision of reasonable and appropriate protection of e-PHI, and update documentation of such security measures.

Exhibit A provides a quick reference guide for the Security Rule's standards and implementation specifications.

VI. FLEXIBILITY OF APPROACH

The Security Rule provides each HIPAA covered entity and business associate with the flexibility to determine how it will meet the Security Rule standards. This means the Organization may design the specific security measures that are reasonable and appropriate in light of its own business operations. In this regard, the Organization has taken into account:

- The Organization's size, complexity, and capabilities.
- The Organization's technical infrastructure, hardware, and software security capabilities.
- The cost of security measures.
- The probability (how likely it would be) and criticality (the scope of damage it would cause) of potential risks to the Organization's e-PHI.

The Organization will continue to monitor these factors, even after particular security measures have been chosen. The Organization will review and modify security measures as necessary to ensure the provision of reasonable and appropriate protection of the Organization's e-PHI.

VII. TECHNOLOGY NEUTRAL

The Security Rule does not establish specific mandates for meeting the security standards. Moreover, the Security Rule does not prescribe the use of specific technology. Accordingly, the Security Rule will continue to apply, even in the face of continuing technological advances.

VIII. REFERENCES

45 C.F.R. § 160.103 (definitions); 45 C.F.R. § 164.302 (applicability); 45 C.F.R. § 164.304 (definitions); 45 C.F.R. § 164.306 (security standards: general rules).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: **ASSIGNED SECURITY RESPONSIBILITY: HIPAA SECURITY OFFICER**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization designates an individual, the HIPAA Security Officer ("Security Officer"), with responsibility for oversight of this HIPAA Security Rule Policy Manual and the Organization's security program. The Organization designates an individual, who may be the Security Officer or some other individual within the Organization, to serve as the HIPAA Privacy officer (the "Privacy Officer"). The Privacy Officer and Security Officer, in conjunction with the Organization's Compliance Committee, are responsible for the development, implementation, oversight and enforcement of the Organization's HIPAA Compliance Program.

The Security Officer shall have authority to carry out his/her responsibilities either directly or through delegation to employed or contracted technical consultants. As such, references in this Manual to a task or tasks to be performed by the Security Officer may mean directly by the Security Officer or through delegation to employed or contracted technical consultants. Any such designated consultants shall report to the Privacy Officer and Security Officer with respect to matters covered under the Organization's HIPAA Compliance Program.

II. PROCEDURES

1. The Security Officer is responsible for the day-to-day operation and management of the Organization's security program and the policies and procedures contained in this HIPAA Security Rule Policy Manual. The Security Officer shall serve as a member of the Compliance Committee, shall report to the Executive Director and shall have direct access to the Organization's Board of Trustees as needed.

2. The Security Officer shall possess the following minimum qualifications and experience:

   (a) Thorough knowledge and understanding of HIPAA, including the HIPAA Privacy Rule and HIPAA Security Rule, as well as state laws and regulations governing the privacy and security of patient information.

   (b) In-depth computer and information system knowledge and skills.

   (c) Experience in project management.

(d) High level of integrity and trust.

(e) Industry-related experience in HIPAA compliance or health care corporate compliance.

3. The Security Officer is charged with the following duties and responsibilities (i.e., job description), as may be amended from time-to-time:

(a) Maintain current knowledge of applicable federal and state laws and regulations governing the privacy and security of patient information, and related to computers, information systems and information technology.

(b) Oversee and monitor the development and implementation of the Organization's Security Rule Policy Manual, and work with the Organization's Privacy Officer in his/her oversight of the Organization's Privacy Rule Policy Manual.

(c) Coordinate activities related to the HIPAA Compliance Program with the Privacy Officer.

(d) Assist the Privacy Officer with workforce HIPAA training, and deliver periodic security reminders and memoranda to the Organization's workforce regarding HIPAA security.

(e) Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Organization's HIPAA Compliance Program.

(f) Maintain an accurate inventory of all information systems, devices and media through which PHI may be accessed, created, maintained and/or transmitted.

(g) Act as the point of contact for the reporting of security concerns, and respond to questions and reports regarding the security concerns.

(h) Identify, prevent, respond to and/or mitigate security incidents and breaches, or other concerns affecting the confidentiality, integrity and availability of e-PHI and implement appropriate administrative, physical and technical safeguards.

(i) Perform or ensure the performance of periodic gap and risk analyses, including documentation thereof and implementation of necessary safeguards, including through collaboration with or delegation to any business associate engaged by the Organization for such purposes.

(j) Report periodically to the Compliance Committee and Board of Trustees concerning the implementation, oversight and enforcement of the Organization's HIPAA Compliance Program.

III. REFERENCES

45 C.F.R. § 164.308(a)(2).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY MANAGEMENT PROCESS

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization, either directly or through the engagement of employed or contracted technical consultants, shall implement reasonable safeguards to ensure the confidentiality, integrity and availability of its information systems and the electronic protected health information, or e-PHI, the Organization creates, receives, maintains or transmits. In addition, the Organization will strive to prevent, detect, contain, mitigate and correct security violations and breaches. The Organization will accomplish these tasks through, in part:

- Performing periodic gap and risk analyses to evaluate potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI and to identify the environmental, financial, legal and technical impact of such risks and vulnerabilities.
- Defining and understanding all information system capabilities and boundaries by conducting ongoing inventory, tracking, upgrading, and disposal of hardware, software, devices and other media and applications containing e-PHI and other Data.
- Implementing and conducting appropriate security measures and controls sufficient to prevent, detect and/or reduce risks and vulnerabilities, and protect against any reasonably anticipated uses or disclosures that are not permitted or required under HIPAA.
- Implementing and conducting procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.
- Appropriately responding to security incidents and breaches.
- Educating the Organization's workforce, and ensuring compliance by the workforce with the Organization's HIPAA Compliance Program.
- Applying appropriate sanctions against workforce members who fail to comply with the Organization's HIPAA Compliance Program.

As used in this Policy, the following terms are defined as set forth below:

"Availability" means the timely, reliable and uninterrupted access and usability of infrastructure and Data.

"Confidentiality" means protecting Data and information and ensuring it is not made available or disclosed to unauthorized persons or processes.

"Data" means any and all information, including but not limited to, individually identifiable health information and PHI.

"Integrity" means that Data or information has not been altered or destroyed in an unauthorized manner.

II. PROCEDURES

1. The Security Officer shall periodically identify relevant information systems that store e-PHI and Data, either temporarily or permanently. All hardware and software that are used to collect, store, process, or transmit e-PHI and Data shall be identified. The results of such inventory shall be documented and maintained by the Security Officer for a period of at least six (6) years from the date of the performance of such inventory.

2. The Security Officer shall periodically analyze business functions and verify ownership and control of information system elements as necessary. The following should be considered:

   (a) Who or what organization is responsible for the specific hardware or software (e.g., HIE Vendor).

   (b) Whether the current information system configuration is documented, including connection to other systems.

   (c) Whether the types of information and uses of that information have been identified and the sensitivity of each type of information evaluated. Each type of Data should be classified with regard to its impact on business operations (essential or critical vs. non-essential), level of security or threat risk, and/or proprietary or confidential nature.

   (d) Whether access to such Data is limited to what is reasonable and necessary given the nature of each type of Data's classification and reasonable and appropriate safeguards applied to prevent unauthorized access.

3. The Security Officer shall work with the Compliance Committee to ensure the performance of periodic risk and gap analyses, at such intervals as determined by the Compliance Committee. For any environmental and other changes affecting or potentially affecting e-PHI or Data (i.e., acquisition of new software, hardware, or applications), gap and risk analyses should be conducted to evaluate the impact of any such changes. Information concerning the conduct of risk analyses is contained in **Exhibit B**.

4. The Security Officer shall work with the Committee to ensure documentation of output and outcomes from the gap and risk analyses, and the development and implementation of a risk management plan to address identified risks and vulnerabilities.

5. The Security Officer shall periodically review risk and gap analyses with the Compliance Committee as reasonably necessary to ensure any identified deficiencies or security measures have been resolved or are in the processes of resolution.

6. The Security Officer shall monitor the performance, access to, and use of all information systems, and assess periodically whether additional hardware, software and/or services may be needed to reasonably and adequately protect e-PHI and Data. As necessary, the Security Officer shall make recommendations to the Executive Director regarding needed hardware, software and technology services.

7. The Security Officer shall develop and implement procedures to regularly review information system activity, such as audit logs, access reports and security incident tracking.

8. The Security Officer shall document all decisions concerning the management, operational, and technical controls selected to identify, evaluate and mitigate identified risks.

9. The Security Officer shall recommend to the Compliance Committeeroles and responsibilities for the implementation of each control to particular individuals or offices, as applicable.

10. The Security Officer shall develop and implement procedures as reasonably necessary to accomplish particular security related tasks necessary and appropriate for the Organization's business operations.

11. All documentation produced by the Security Officer under this policy shall be retained for a period of at least six (6) years.

III. REFERENCES

45 C.F.R. § 164.308(a)(1)

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: WORKFORCE SECURITY

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to ensure that all applicable members of its workforce have appropriate access to electronic protected health information, or e-PHI, and to prevent those who do not need access from obtaining it. The following procedures shall be performed by or through delegation at the direction and under the supervision of the Security Officer.

II. PROCEDURES

1. The Security Officer shall develop and maintain, at all times, a complete and accurate listing of all members of the Organization's workforce, their job descriptions, and the circumstances in which each individual workforce member needs access to e-PHI in order to perform his/her job functions. The list may be by individual or by job category.

2. The Security Officer shall ensure that all individuals who need access to e-PHI to perform each individual's job functions are trained in the Organization's technology and security requirements.

3. The Security Officer shall communicate to each workforce member whether or not he/she is permitted to access e-PHI. Any workforce member given permission to access e-PHI shall only do so when, and to the extent, necessary to perform job functions. Any workforce member not given express permission to access e-PHI is prohibited from doing so.

4. The Security Officer shall implement termination procedures to be followed upon termination of employment or engagement of any workforce member, in order to terminate access to e-PHI and information systems. In addition, workforce members shall be required to return to the Organization:

    (a) Identification badges;

    (b) Door keys, access cards, swipe cards and similar access instruments and devices;

    (c) File cabinet keys;

(d) All electronic devices and media belonging to the Organization, and all devices and media containing e-PHI or other Organization information;

(e) Any other equipment or items belonging to the Organization.

5. The Security Officer shall terminate passwords, user identification codes and other logon codes upon termination of a workforce member's employment or engagement with the Organization, to ensure such workforce member may no longer access e-PHI or information systems, either on-site or remotely.

III. REFERENCES

45 C.F.R. § 164.308(a)(3).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: INFORMATION ACCESS MANAGEMENT

Date Adopted: May 1, 2020

Revised:

I. POLICY

The purpose of this Policy is to outline the Organization's procedures for granting authorization for access to electronic Protected Health Information, or e-PHI, by workforce members.

II. PROCEDURES

1. Access Authorization. The Security Officer, in consultation with the Privacy Officer and relevant management, shall:

   (a) Assess how access to e-PHI, workstations, information systems, programs, processes and applications will be determined.

   (b) Determine restrictions on access, which should be *identity-based, role-based, location-based, or some combination thereof*, and consistent with other existing management, operational and technical controls.

   (c) Establish standards for granting access. Formal authorization should be obtained from the Security Officer or her/his designee, before access to e-PHI, workstations, information systems, programs, processes and applications is granted to any user. If possible in the capabilities of the Organization's systems, only the minimum necessary e-PHI should be made available to each workforce member based on his/her job requirements and on a need-to-know basis.

   (d) Maintain a log of workforce members with access rights, including specific rights granted.

2. Access Establishment and Modification. The Security Officer, in consultation with the Privacy Officer and relevant management, shall:

   (a) Implement procedures to establish, document, review, modify and remove a user's right of access to e-PHI, workstations, information systems, programs, transactions, processes and applications.

(b) Evaluate access controls already in place or implement new access controls as reasonably appropriate and as needed, both periodically and on a routine basis.

(c) Coordinate with management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.

III. REFERENCES

45 C.F.R. § 164.308(a)(4).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY AWARENESS & TRAINING

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization will train all members of its workforce on the policies and procedures that comprise the Organization's HIPAA Compliance Program as necessary and appropriate for the purpose of carrying out each workforce member's job functions. New workforce members will receive training within a reasonable period of time after joining the Organization, and all workforce members will receive periodic training. Training will be conducted by or under the direction of the Privacy Officer and Security Officer.

II. PROCEDURES

1. The Privacy Officer shall be responsible, either directly or through delegation, for developing and updating, as needed, training resources and for ensuring implementation of privacy training to workforce members. At minimum, topics will include:

    - Uses and disclosures of patient information
    - Individual privacy rights
    - Privacy breaches and reporting responsibilities
    - Business associate relationships
    - Sanctions for violations of the requirements set forth in the Organization's HIPAA Compliance Program and/or HIPAA and other privacy laws.

2. The Security Officer shall be responsible, either directly or through delegation, for developing and updating, as needed, training resources and for ensuring implementation of security training to workforce members. At minimum, topics will include:

    (a) *Security Reminders.* The Security Officer shall ensure that periodic security reminders are provided to all workforce members as reasonable and appropriate to advise about changes in the laws and regulations regarding security and in organizational policies or procedures, and to warn about or correct ongoing security concerns, threats, vulnerabilities or violations concerning the confidentiality, integrity and availability of electronic PHI.

    (b) *Password Management.* The Security Officer shall ensure that workforce members are educated on appropriate password creation, maintenance and

confidentiality, including selecting "strong passwords," periodically changing passwords, not sharing passwords with any workforce member or other individual, and not writing down passwords.

(c) *Protection from Malicious Software*. The Security Officer shall ensure that workforce members are educated in applications and mechanisms for safeguarding information systems and electronic PHI from malicious software or attacks, such as a virus, malware, hacking, ransomware or other security incident, and for appropriate reporting mechanisms regarding the same.

(d) *Log-in Monitoring.* The Security Officer shall ensure that workforce members are educated on the Organization's processes for monitoring all log-ins and log-in attempts, procedures for temporarily suspending access after failed log-in attempts, and procedures required to re-activate access after failed log-in attempts.

(e) *Mobile Devices and Portable Media.* The Security Officer shall ensure that workforce members are appropriately educated on the privacy and security risks associated with mobile devices and portable media through which PHI may be created, maintained, accessed or transmitted, and for following the Organization's procedures for the same.

3. Each workforce member will certify that he/she received training and understands the Organization's HIPAA Compliance Program and the requirements of HIPAA. The Organization will maintain training materials and proof of training records for a period of at least six (6) years.

III. REFERENCES

45 C.F.R. § 164.308(a)(5).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: SECURITY INCIDENT PROCEDURES

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization treats Security Incidents with the highest concern and regard and shall take action to identify and address Security Incidents as soon as reasonably practicable.

A **Security Incident** includes any **attempted** *or* **successful** unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the Organization's information systems.

The Organization shall take such steps as reasonable and necessary to:

- *Detect and Identify* Security Incidents;
- *Investigate* and *Evaluate* Security Incidents;
- *Respond* to Security Incidents as reasonable and appropriate;
- *Mitigate* any harmful effects from Security Incidents, to the extent reasonably practicable; and
- *Correct and Prevent* subsequent similar or dissimilar Security Incidents.

II. PROCEDURES

1. Detection and Identification.

   (a) All workforce members, agents and business associates of the Organization shall report any potential/suspected or actual/known Security Incident to the Privacy Officer or Security Officer ***as soon as possible and without delay***.

   (b) By way of example, the types of incidents to report include, but are not limited to, the following:

      (i) Any event in which access to electronic protected health information ("e-PHI") or other information within the Organization's information systems might have been gained by an unauthorized person.

      (ii) Any event in which a device containing (or may be containing) PHI or other information within the Organization's information systems has (or might have been) lost, stolen or infected with a virus or malicious software.

(iii) Any emails received within the Organization's system containing suspicious attachments or links or other suspicious information.

2. Investigation and Evaluation.

(a) The Organization shall investigate all reported or discovered Security Incidents. The Security Officer shall investigate, gather and document all information relating to the facts and circumstances of a Security Incident.

(b) The Organization shall promptly evaluate all reported incidents to determine whether a given Security Incident rises to the level of a breach of unsecured PHI. Reference is made to the policies entitled, "Breaches of Information – HIPAA" and "Breaches of Information – New Jersey Identity Theft Prevention Act," in the Organization's HIPAA Privacy Rule Policy Manual.

(c) The Organization shall document and retain all of the information obtained through investigation and evaluation concerning a Security Incident for a period of at least six (6) years.

3. Response.

(a) The Organization shall respond to any reported or discovered Security Incident, including, but not limited to, implementing corrective and mitigating action and imposing sanctions against violating persons or business associates when appropriate.

(b) The Organization shall respond to any Security Incident that is reasonably believed to be a breach of unsecured PHI in accordance with the Organization's policies entitled "Breaches of Information – HIPAA" and "Breaches of Information – New Jersey Identity Theft Prevention Act," in the Organization's HIPAA Privacy Rule Policy Manual.

4. Correction, Mitigation and Prevention. The Organization shall take reasonably necessary steps to mitigate the harmful effects, as far as reasonably practicable, of any Security Incident and/or breach of unsecured PHI, including evaluative, disciplinary, and other corrective action as may be appropriate to decrease the risk of harm and/or prevent re-occurrence of the Security Incident and/or breach of unsecured PHI, and implementing additional or modifying processes and procedures as may be reasonably necessary to address identified security gaps.

III. REFERENCES

45 C.F.R. § 164.308(a)(6).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: CONTINGENCY PLANS

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to establish Contingency Plans in order to protect the confidentiality, integrity, availability and accessibility of the Organization's electronic protected health information ("e-PHI") from vulnerability in the event of an extraordinary event or emergency (e.g., fire, vandalism, system failure or natural disaster) and to enable sustained operation of the Organization's information systems if such event or emergency damages systems that contain e-PHI.

II. PROCEDURES:

1. Data Back-Up Plan. The Organization shall establish and implement procedures to create and maintain retrievable exact copies of e-PHI. The Organization's Data Back-Up Plan is contained in **Exhibit C**.

2. Disaster Recovery Plan. The Organization shall establish, and implement as needed, procedures to restore any loss of data in the event of an extraordinary event or emergency (e.g., fire, vandalism, system failure or natural disaster), or other occurrence that results in the destruction of or damage to e-PHI. The Organization's Disaster Recovery Plan is contained in **Exhibit D**.

3. Emergency Mode Operation Plan. The Organization shall establish, and implement as needed, procedures to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode. In the event of any unforeseen occurrence that affects the Organization's ability to continue with its standard operating procedure, the Organization shall take the following measures: (a) declare the event an emergency; (b) activate emergency mode; (c) assess damage and implement the plan; and (d) recover/restore business operations. The Organization's Emergency Mode Operation Plan is contained in **Exhibit E**.

4. Testing and Revision Procedures. The Organization shall implement procedures for periodic testing and revision of Contingency Plans. In the event any deficiencies in the plans are discovered, the plans will be revised accordingly.

5. Applications and Data Criticality Analysis. The Organization shall assess the relative criticality of specific applications and data in support of other Contingency Plan components, including the criticality, vulnerability and security of the

Organization's programs and information. Such assessment shall be modified, as necessary, to account for changes to the Organization's infrastructure. The assessment shall take into consideration the length of time the system or data can be inaccessible before the Organization suffers an unacceptable negative impact. Such analyses may be included in the Organization's Disaster Recovery Plan or maintained separately.

III. REFERENCES

45 C.F.R. § 164.308(a)(7).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: EVALUATION OF SECURITY POLICIES

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to perform a periodic technical and non-technical evaluation of its HIPAA Security Rule Policies and Procedures based on HIPAA, as it may be amended from time to time, and in response to environmental or operational changes affecting the security of electronic protected health information, or "e-PHI," to ensure continued compliance with the HIPAA Security Rule.

II. PROCEDURES

1. The Compliance Committee shall monitor changes to the HIPAA privacy and security statutes and regulations, and any governmental guidance related thereto, and shall recommend revisions to this Manual as needed.

2. The Security Officer, in conjunction with the Compliance Committee, shall periodically, at such intervals as determined by the Compliance Committee, review the policies and procedures contained in this Manual for compliance and effectiveness. Such review also shall be performed as soon as possible after any material environmental or operational changes affecting the security of e-PHI, or when there is a change in applicable laws and regulations.

3. The Organization shall conduct periodic risk and gap analyses in accordance with the policy in this Manual entitled "Security Management Process."

III. REFERENCES

45 C.F.R. § 164.308(a)(8).

HIPAA SECURITY POLICIES:
ADMINISTRATIVE SAFEGUARDS

Topic: HIPAA BUSINESS ASSOCIATES

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to have a written business associate agreement in place with each of the Organization's business associates. If a business associate uses a subcontractor to perform certain functions for the Organization on behalf of the business associate, then the business associate must enter into a written business associate agreement with the subcontractor.

II. PROCEDURES

1. The Privacy Officer, together with the Security Officer, shall ensure that the Organization enters into a written business associate agreement with each of its business associates. The Security Officer and Privacy Officer also shall require each business associate to enter into a written business associate agreement with any subcontractor that performs services for the Organization on behalf of the business associate.

2. For additional requirements for business associate agreements, please refer to the policy in the HIPAA Privacy Rule Policy Manual entitled "Business Associates."

III. REFERENCES

45 C.F.R. § 164.308(b)(1).

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: FACILITY ACCESS CONTROLS

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to implement policies and procedures to limit physical access to electronic information systems and to its facilities in which such systems are housed, while ensuring that properly authorized access is allowed.

Facility access controls are accomplished through:

- Contingency Operations – Procedures that allow facility access in support of restoration of lost data under the Organization's Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

- Facility Security Plan – Policies and procedures to safeguard the Organization's facilities and equipment in its facilities from unauthorized physical access, tampering and theft.

- Access Control and Validation Procedures – Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

- Maintenance Records – Policies and procedures to document repairs and modifications to the physical components of the Organization's facilities which are related to security (e.g., hardware, walls, doors and locks).

II. PROCEDURES

1. Contingency Operations. In the event the Organization experiences an emergency or disaster causing a disruption of access to systems, the procedures set forth in the policy in this Manual entitled, "Contingency Plans," (and the related policies referenced therein) shall be followed. The Executive Director of the Organization shall determine the individuals who shall be granted facility access during and after such event until full operations are restored. In addition, the Executive Director of the Organization shall make the determination that full operations have been restored.

2. Facility Security Plan. In order to safeguard the Organization's facilities and equipment in the Organization's facilities from unauthorized physical access,

tampering and theft, the following procedures shall be established and followed in the Organization:

(a) In order to promote and ensure overall security, the Organization shall implement controls to restrict physical access to its facilities and on-site electronic information systems to ensure access to non-public areas is granted to authorized individuals only. As part of these controls, the Organization shall categorize areas within its facilities as either "public" or "restricted." This categorization may be permanent or variable based on outside factors such as the date or time (e.g., an area may be designated public during normal business hours but restricted outside of normal business hours). Areas housing electronic systems shall be considered restricted at all times.

(b) All entrance locations, doors and windows must be secured by the person primarily responsible for such activities. The Organization shall designate an individual or individuals responsible for ensuring all entrance locations, doors and windows are properly secured or locked to prevent unauthorized access.

(c) The Organization shall implement procedures to ensure that electronic systems within Organization are physically accessible only to authorized individuals. Workstations should be set up in a manner to prevent public access or viewing.

(d) The Organization shall implement procedures to ensure that all hardware, network connections, software, data and other electronic files are, as much as possible, stored away from potential natural physical hazards, such as water/cooling/heating pipes, vents or ducts, any visible signs of water/cooling/heating or other natural damage, direct sunlight and extreme heat or cold.

(e) The Organization shall implement procedures to ensure that air vents on computers and other heat-producing equipment will not be covered or restricted, causing inadequate air flow so as to avoid a fire hazard.

(f) The Organization shall implement procedures to ensure that electrical circuits are not overloaded, and that additional circuits are installed if needed. Power strips may be used when necessary, but must be used individually and not plugged into each other. Electrical equipment with defective cords must be taken out of service promptly and replaced.

(g) The Security Officer will establish protocols for the Organization to inspect computers and other electronic information systems on a periodic basis.

3. Access Control and Validation.

(a) Public areas are considered accessible, during normal business hours, by the general public.

(b) Access to areas housing electronic equipment, systems or information shall be limited to those individuals authorized by the Organization and who have a legitimate need for such access. Computer and other electronic systems shall be located in areas capable of being monitored and supervised, and that may be locked or otherwise secured during non-business hours or when otherwise incapable of being monitored and supervised.

(c) Access to software programs for testing and revision shall be strictly limited to the individual(s) specifically designated and authorized by the Security Officer.

4. Maintenance Records. The Organization shall ensure access to areas housing or containing computers and electronic systems by maintenance and repair personnel is carefully monitored and supervised. The Organization shall maintain repair and maintenance logs or records documenting repairs, maintenance and modifications to the physical components of the Organization's facilities which are related to security (e.g., hardware, walls, doors and locks). Documentation shall be maintained for a period of at least six (6) years.

III. REFERENCES

45 C.F.R. § 164.310(a)(1).

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: WORKSTATION USE

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization has established policies and procedures related to workstation use that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access or that houses electronic protected health information, or "e-PHI."

II. PROCEDURES

1. Generally. The Security Officer, in conjunction with the Compliance Committee, will establish guidelines for workstation use to promote reasonable security in the handling of electronic systems and e-PHI. The Security Officer is responsible for ensuring that workforce members are advised and instructed on the proper set-up, use and security safeguards for individual workstations, computers and devices.

2. Operating Environment.

   (a) All computers owned by the Organization have been configured according to standards established by the Organization, and all configurations, software and programs are the sole property of the Organization. All data contained in the Organization systems (including in local drives and on media) is the sole property of the Organization, whether inputted for work or personal use. Personal use of the Organization's computers and systems is not permitted. No workforce member (other than the Security Officer and System Administrator) is authorized to change any settings on computers or systems without the express permission and instructions of the Security Officer or System Administrator.

   (b) Only software or application programs authorized by the Security Officer may be installed or loaded onto the Organization's information system or any terminal. Unless specifically authorized and instructed by the Security Officer or System Administrator, no workforce member is authorized to install or download any software or programs onto the Organization computers or systems. Suspicions or concerns regarding malicious software, viruses, worms, etc. must be reported to the Security Officer immediately.

(c) Only designated workforce members assigned to work functions relating to e-PHI or otherwise authorized electronic functions may operate computer terminals, software or systems.

(d) All computers owned by the Organization will be connected to surge protectors.

(e) Workforce members are expected to monitor their own workstations and must report potential threats to internal or external systems to the Security Officer.

(f) Workforce members should keep computer terminals, hard drives, keyboards, and screens clear of food and liquids at all time.

3. Passwords.

(a) Workforce members are expected to maintain the confidentiality of their passwords and are responsible for the security of their passwords.

(b) Workforce members may log onto the Organization's systems only with their own passwords. Under no circumstances may a workforce member share his/her password with another workforce member or unauthorized person. System access will be monitored by or under the direction and supervision of the Security Officer.

4. Content.

(a) Workforce members may use the Organization's computers, email system, fax machines, printers and other systems for work-related purposes only. All content is the sole property of the Organization.

(b) Workforce members will be held responsible for the content of any data entered into the system. This includes any information transmitted within or outside the Organization. A workforce member will not hide his/her identity as the author of any entry or represent that someone else entered the data or sent the message.

5. Automatic Log-Off. The Security Officer will determine the timing of automatic log-off of workstations after a period of inactivity. No workforce member is permitted to turn off, override or otherwise interfere with automatic log-off settings.

6. Electronic Mail.

(a) The Organization's email system may be used only for work-related purposes. The Organization, either directly or through delegation to its System Administrator, reserves the right to monitor email usage.

(b) No pictures, graphics, movies or email attachments may be opened, downloaded, stored, saved or otherwise placed onto the Organization's

computers and systems, unless specifically authorized for the Organization's business purposes.

(c) Forgery (or attempted forgery) of email messages is prohibited.

(d) Any attempt to read, delete, copy, or modify the email of other users is prohibited.

(e) Sending junk email, "for-profit" email or chain email on or through the Organization's computers or systems is prohibited.

(f) Sending harassing, obscene, bullying or threatening email to another is strictly prohibited.

(g) Extreme caution should be exercised prior to opening email attachments from unknown senders, which may contain viruses. Workforce members should contact the Security Officer or System Administrator prior to opening any suspicious email attachments, in order to seek guidance.

7. Internet Access.

(a) The Organization authorizes the availability of the Internet to provide access to Internet resources that will enhance and support business activities. It is expected that workforce members will use the Internet to improve their job knowledge and to access information on topics that have relevance to the Organization's operations.

(b) Workforce members should be aware that when access is accomplished using Internet addresses and domain names registered to the Organization, they may be perceived by others to represent the Organization. Users are advised not to use the Internet for any purpose that would reflect negatively on the Organization or its workforce.

(c) Workforce members are prohibited from accessing and using the Internet utilizing the Organization's computers, systems or facilities for any of the following:

(i) Accessing, retrieving, or printing text and graphics information that exceeds the bounds of generally accepted standards of good taste and ethics.

(ii) Engaging in any unlawful activities or any other activities that would in any way bring discredit to the Organization.

(iii) Engaging in any activity that would compromise the security of the Organization's systems or facilities.

(iv) Obtaining personal files via the Internet on individual PC hard drives or on local area network (LAN) file servers.

(v) Game playing of any kind.

(vi) Propagating any computer virus.

(vii) Maintaining a secret pass code.

(d) Workforce members will follow existing security policies and procedures in their use of Internet services and will refrain from any practices that might jeopardize the computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

(e) The Organization, either directly or through delegation to its System Administrator, reserves the right to monitor Internet usage.

8. Remote Access. Remote access means any access to the Organization's network through a non-Organization controlled device, whether on-site or off-site.

(a) Remote access is permitted only with the express permission of the Organization.

(b) Authorized remote users are required to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Organization. Remote users must not obtain access through publicly-available wi-fi or other internet connections.

(c) Remote users must ensure their remote connection is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

(d) Secure remote access must be strictly controlled. Control will be enforced via password authentication.

(e) At no time should any workforce member provide his/her login or email password to anyone, not even family members.

(f) Remote access must not be used for personal email accounts (i.e., Gmail, Hotmail, Yahoo, AOL) or other external resources to conduct Organization business, thereby ensuring that official business is never confused with personal business.

(g) Reconfiguration of a remote user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

(h) All hosts that are connected to the Organization's internal networks via remote access technologies must use the most up-to-date anti-virus software.

III. REFERENCES

45 C.F.R. § 164.310(b).

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: WORKSTATION SECURITY

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization that only authorized functions may be performed on the Organization's workstations. The Organization strives to ensure that appropriate physical safeguards are utilized for all workstations to prevent access to electronic protected health information ("e-PHI") by unauthorized users.

II. PROCEDURES

1. The Security Officer will work with the Organization in order for the Organization to:

   (a) Identify all methods of physical access to workstations (including workstations located in public areas and laptops that are used as workstations).

   (b) Identify physical safeguards in place (e.g., locked doors, cameras, receptionist), identify any gaps in such safeguards and add additional safeguards as deemed appropriate.

2. Computer terminals should be positioned to avoid or minimize the likelihood of public viewing or viewing by non-authorized individuals. If necessary and possible, workstations should be relocated to secure areas.

3. If possible, workstations should be physically locked to ensure unauthorized access.

4. Privacy screens and screensavers should be used if and when possible.

III. REFERENCES

45 C.F.R. § 164.310(c).

HIPAA SECURITY POLICIES:
PHYSICAL SAFEGUARDS

Topic: DEVICE AND MEDIA CONTROLS

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information ("e-PHI") into and out of the Organization, and the movement of these items within the Organization.

II. PROCEDURES

1. Disposal. The Organization shall ensure that disposal of hardware and electronic media containing e-PHI is monitored and handled in accordance with this Policy and the procedures required by the Security Officer.

   (a) E-PHI must be deleted from hardware and electronic media when there is no longer a business or clinical need to access and use such information, and prior to such hardware or media being disposed or otherwise taken out of use. Only authorized personnel may delete e-PHI. The Security Officer will oversee all deletion procedures.

   (b) Hard drives of computers must be reformatted, purged, permanently wiped or destroyed before being discarded or before being sold or returned to a leasing company or vendor. The Security Officer will oversee all procedures relating to reformatting, purging, permanently wiping or destroying hard drives.

   (c) The disposal of hardware and electronic media containing e-PHI into dumpsters, recycling bins, trash receptacles or in any other manner except as provided under this Policy is strictly prohibited.

   (d) The Security Officer will ensure disposal procedures are in compliance with current industry standards.

2. Media Re-Use. All e-PHI residing in media must be permanently deleted, wiped and removed prior to re-use.

   (a) Workforce members must return all media containing e-PHI to the Security Officer, prior to re-use.

(b) The Security Officer will oversee procedures to ensure media containing e-PHI is permanently deleted, purged, wiped and removed prior to issuing the media for re-use.

3. Accountability. The Security Officer will manage, either directly or through delegation, the movement of hardware and electronic media in and out of the Organization.

(a) The Security Officer will oversee procedures to ensure the accountability of hardware and electronic media at the Organization.

(b) No hardware or electronic media will be brought into or removed from the Organization without the prior approval of the Security Officer or individual(s) designated by the Security Officer.

(c) The Security Officer will develop a system for logging and monitoring the movement of hardware and electronic media.

4. Data Backup and Storage. The Security Officer will oversee procedures to ensure that a retrievable, exact copy of e-PHI exists or is created prior to the movement of any hardware or electronic media containing e-PHI.

III. REFERENCES

45 C.F.R. § 164.310(d)(1).

HIPAA SECURITY POLICIES:
TECHNICAL SAFEGUARDS

Topic: ACCESS CONTROL

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization implements technical policies and procedures for electronic information systems that maintain electronic protected health information ("e-PHI") to allow access only to those persons or software programs that have been granted access rights as specified under the Policy in this Manual entitled "Information Access Management." The scope and manner of such access shall be as determined by the Security Officer and the Compliance Committee.

II. PROCEDURES

1. Assessment & Evaluation. The Security Officer shall:

   (a) Identify the applications and systems that require access controls, with a focus on the applications and systems housing e-PHI.

   (b) With respect to all applications, systems and data where it has been determined that access control is required, determine the ***scope and degree*** of access control needed (e.g., *How is the system being accessed: Is the data and/or system being accessed remotely? Is the data being viewed only? Is the data being modified? Is new data being created and stored on the system?*).

2. Unique User Identifier & Password. The Security Officer shall:

   (a) Assign a unique user identifier to each systems user, which must be used each time the user logs into a computer or software that houses e-PHI. Each user must keep his/her unique user identifier private and confidential. No user may log into a computer or software using another person's unique user identification number.

   (b) Ensure that system activity can be traced to a specific user (e.g., record entries, modifications, deletions made by physicians, or made by nurses and other clinical or administrative staff) and ensure that the necessary data is available in the system logs to support audit and other related business functions.

(c) Set password requirements and controls (e.g., requiring system users to choose passwords with combination of symbols, letters and numbers, and minimum password length of 7 characters).

3. Emergency Access Procedure. The Security Officer shall:

(a) Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems or emergency.

(b) Activate emergency access procedures when necessary, granting authority to designated individuals to access systems to continue critical functions until the emergency is managed or terminates.

4. Automatic Log-Off. The Security Officer shall implement procedures and systems necessary to cause automatic termination of an electronic session after a pre-determined period of inactivity. The timing of log-off shall be as determined by the Security Officer.

5. Encryption and Decryption. The Security Officer shall install, manage and oversee the effectiveness and functionality of encryption and decryption software. The Security Officer shall institute policies and procedures to ensure that e-PHI sent electronically outside the Organization's secure electronic environment are sent utilizing encryption software. Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

III. REFERENCES

45 C.F.R. § 164.312(a)(1).

Topic: **AUDIT CONTROLS**

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to implement hardware, software, and/or procedural mechanisms that record and examine activity in the Organization's information systems that contain or use electronic protected health information ("e-PHI").

II. PROCEDURES

The Security Officer, in conjunction with the Compliance Committee, shall:

1. Determine how decisions on audits and reviews shall be made, who is responsible for the overall audit process and results, the frequency of audits, and how they will be analyzed.

2. Conduct a risk analysis to identify the systems or activities that the Organization will track or audit as well as current technological infrastructure, hardware and software capabilities. Refer to the Policy in this Manual entitled "Security Management Process."

3. Determine the appropriate scope for identified system audits.

4. Conduct routine and periodic audits to assess, monitor and evaluate information systems, compliance by workforce members, the occurrence of unauthorized accesses, and any potential or actual security incidents.

5. Maintain audits logs that collectively track and monitor information systems, user activity and data accessed and disclosed by workforce members. Audit activity shall be maintained within the defined capabilities of each system and/or application but at a minimum must include:

   (a) Date and time of login/logout or login attempt;

   (b) Identified failed logins and system lock-outs;

   (c) Source/type of information system or data which was accessed;

   (d) Identity of the user, including where applicable and available, the action which was taken; and

(e) Identity of the individual whose data was accessed.

6. Audit logs shall be unchangeable and reviewed periodically on a schedule as established by the Security Officer in consultation with the Compliance Committee. Any suspect activity or potential security incident shall be reported promptly to the Security Officer. Existing system capabilities and tools for auditing shall be evaluated for effectiveness by the Security Officer in consultation with the Compliance Committee. Upgrades shall be implemented when deemednecessary.

7. Review and utilize results of the risk analyses to determine which systems and activities should be tracked and audited, and to monitor the need for additional audit capabilities and security controls.

8. Ensure that workforce members are appropriately informed on accountability through the audit processes, and that they are trained on how the review/audit policy could impact their job responsibilities and employment status.

9. Address processes for reviewing exception reports, where the monitoring reports will be filed and maintained, whether there is a formal process in place to address system misuse, abuse and fraudulent activity and how appropriate workforce members will be notified regarding suspect activity.

10. Audit logs shall be maintained for a period of six (6) years from the date on which the e-PHI/data is accessed.

III. REFERENCES

45 C.F.R. § 164.312(b).

HIPAA SECURITY POLICIES:
TECHNICAL SAFEGUARDS

Topic: INTEGRITY

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization implements policies and procedures to protect electronic protected health information ("e-PHI") from improper alteration or destruction.

II. PROCEDURES

The Security Officer shall institute procedures to safeguard the integrity of e-PHI, including through the following mechanisms:

1. Identifying all users who have been authorized to access e-PHI and all approved users with the ability to create, alter and/or destroy data.

2. Identifying any possible unauthorized sources that may be able to intercept the information and modify it, including identifying scenarios that may result in modification to the e-PHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).

3. Establishing, as applicable, that data is being verified and routed properly, in conformance with protocol or message standards, and assessing whether data quality and transmission is safeguarded, determining as appropriate, necessary implementation schedules for encryption and other appropriate mechanisms.

4. Establishing a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.

5. Implementing ongoing procedures to address these requirements. Identifying which methods will be used to protect e-PHI from modification. Identifying tools and techniques to be developed or procured that support the assurance of integrity.

6. Installing and enabling encryption software, security software, firewalls and anti-virus and anti-malware software, and ensuring same are up to date.

7. Monitoring processes to assess and "audit" effectiveness of integrity safeguards.

8. Ensuring users do not share passwords, and that they log-off all systems and applications when they are not in use.

9. Reassessing integrity processes continually as technology and operational environments change, to determine if they need to be revised.

III. REFERENCES

45 C.F.R. § 164.312(c)(1).

HIPAA SECURITY POLICIES:
TECHNICAL SAFEGUARDS

Topic: PERSON OR ENTITY AUTHENTICATION

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to implement procedures to verify that a person or entity seeking access to electronic protected health information ("e-PHI") is the one claimed.

II. PROCEDURES

1. Authentication for System Access. The identity of all individuals, devices and systems seeking access to the Organization's information systems shall be verified prior to any such individual, device or system being granted access to electronic systems maintained by the Organization. At a minimum, the Security Officer shall:

   (a) Identify technological methods available for authentication. Authentication is the process of establishing the validity of a transmission source or verifying an individual's authorization claim for specific access privileges to information and information systems.

   (b) Select and implement appropriate authentication methods for devices and systems. All devices which may have access to systems and e-PHI, locally or remotely, shall be identified, authorized and authenticated by type, specific device or any combination thereof, prior to being granted access. The Security Officer shall weigh the advantages and disadvantages of authentication approaches in determining what authentication options are reasonable and appropriate for implementation given the Organization's operational and business purposes and electronic information maintained by the Organization.

   (c) Evaluate authentication options available. All users who may create, modify, read or otherwise access electronic systems shall be appropriately authorized and authenticated by use of unique identifiers and passwords. Consider the following options:

      (i) Multi-Factor Authentication – The system will require the user to enter something the user "knows" and something the user "has."

      (ii) Single-Factor Authentication – The system will require the user to enter password and identifier/username.

(d) Evaluate methods periodically as needed, and update or revise as reasonably appropriate based on the availability or appropriateness of additional or alternative authentication mechanisms.

2. Authentication for System Entries/Transmissions. The Security Officer shall:

(a) Require users to comply with username and password requirements, and report lost or compromised credentials immediately to the Security Officer. The Security Officer shall have in place procedures to reestablish lost, corrupted or damaged authentication credentials, and for revoking authentication credentials as necessary.

(b) Require all individuals entering e-PHI to authenticate their credentials when logging onto systems.

(c) Require feedback of authentication information to be obscured to prevent unauthorized individuals from accessing it.

(d) Monitor all access points, whether wireless or local, to guard against tampering, intrusion or damage.

III. REFERENCES

45 C.F.R. § 164.312(d).

HIPAA SECURITY POLICIES:
TECHNICAL SAFEGUARDS

Topic: TRANSMISSION SECURITY

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to implement technical security measures to guard against unauthorized access to electronic protected health information ("e-PHI") that is being transmitted over an electronic communications network.

II. PROCEDURES

1. All transmissions of e-PHI from the Organization to an outside network should utilize an encryption mechanism between the sending and receiving entities, or the file, document or folder containing e-PHI should be encrypted before transmission. (See Section II.6, below.)

2. Prior to transmitting e-PHI to an outside network, the receiving person or entity must be authenticated.

3. All transmissions of e-PHI should include only the minimum amount of PHI necessary for the disclosure.

4. Emails containing e-PHI, whether in the body or in an attachment, should contain a confidentiality statement, such as:

> The information contained in this email and any attachments are private and confidential. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying or the taking of any action in reliance of such information is strictly prohibited. If you have received this email in error, please delete and destroy the information immediately and immediately notify the sender via telephone or return mail.

5. The transmission of e-PHI to an individual via email or other type of messaging system is permitted if the sender has ensured the following conditions are met:

   (a) Encryption (or other method to render e-PHI unreadable, unusable or indecipherable to unauthorized individuals) is utilized, if and whenever possible.

(b) If encryption (or other method to render e-PHI unreadable, unusable or indecipherable to unauthorized individuals) is not possible or the individual has requested to receive communication via unencrypted email or messaging system, the individual has been advised in writing of the risks associated with transmitting e-PHI via email or messaging systems, and has nonetheless consented in writing (e.g., by responsive email or other writing) to receipt by such method.

(c) The receiving individual's identity has been authenticated.

(d) The e-PHI sent via unencrypted email or messaging is the minimum amount of information necessary to comply with the request.

III. REFERENCES

45 C.F.R. § 164.312(e)(1).

HIPAA SECURITY POLICIES:
USE OF MOBILE DEVICES

Topic: USE OF MOBILE DEVICES

Date Adopted: May 1, 2020

Revised:

I. POLICY

It is the policy of the Organization to take measures to protect and secure Protected Health Information, or "PHI," that may be accessed, received, viewed, transmitted or stored on mobile devices, including but not limited to cellular phones, tablets, laptops and other portable devices. The Organization will periodically evaluate and implement measures to address or reduce the risks associated with the use of mobile devices, including, but not limited to, the risks of lost or stolen mobile devices, inadvertent downloading of viruses or other malware, unintentional disclosure to unauthorized users and using unsecured Wi-Fi networks.

II. PROCEDURES

1. Only users authorized by the Executive Director and Compliance Officer may access, receive, view, transmit or store PHI on mobile devices.

2. Mobile device users must take measures to protect and secure PHI when using such devices, whether on-site at the Organization, at a remote work location, or when at home or in public. Users must maintain physical control of devices at all times, including by keeping the device physically in the person's possession and ensuring the device is stored in a secure location when not physically in the person's possession.

3. All mobile devices used to access, receive, view, transmit or store PHI must be password-protected. Users are not authorized to share passwords with or reveal passwords to others, except the Security Officer or System Administrator.

4. The Organization shall implement measures to enhance the security of mobile devices used by workforce members to access, review, view, transmit or store PHI, including any or all of the following:

    (a) Installing and enabling encryption software.

    (b) Installing and enabling a firewall.

    (c) Installing and enabling security software, and keeping security software up to date.

(d) Installing and activating wiping and/or remote disabling capabilities.

(e) Implementing procedures to disable or prohibit the installation of file-sharing applications.

(f) Disposal and re-use of mobile devices shall be subject to the policy in this Manual entitled "Device and Media Controls."

5. PHI accessed, reviewed, viewed, transmitted or stored on mobile devices shall not replace or supersede the medical record. Downloading of any information, including PHI from mobile devices onto the Organization systems is prohibited, except with the express permission of the Privacy Officer or Security Officer. Any needed integration of data on mobile devices onto the Organization's systems shall be performed by or under the supervision of the Security Officer.

III. REFERENCES

healthit.gov website:

Managing Mobile Devices in Your Health Care Organization, **https://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf**

Mobile Devices: Know the Risks. Take the Steps. Protect and Secure Health Information, **https://www.healthit.gov/sites/default/files/mobile_devices_and_health_information_privacy_and_security.pdf**

A Guide to Understanding Your Organization's Mobile Device Policies and Procedures, **https://www.healthit.gov/sites/default/files/fact-sheet-a-guide-to-understanding-your-organizations-mobile-device-policies.pdf**

HIPAA SECURITY POLICIES:
SANCTIONS FOR VIOLATIONS OF HIPAA
COMPLIANCE POLICIES AND PROCEDURES

Topic: **SANCTION POLICY**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization has adopted this Sanction Policy to comply with the requirements of HIPAA as well as to fulfill the Organization's duty to protect the confidentiality, security, integrity, availability and accessibility of Protected Health Information received, maintained, used and disclosed by the Organization. All workforce members are expected and required to follow and comply with the policies and procedures contained in the Organization's HIPAA Privacy Rule Policy Manual and HIPAA Security Rule Policy Manual. These Manuals together comprise the Organization's HIPAA Compliance Program. The Organization will not tolerate violations of its HIPAA Compliance Program policies and procedures, and violations will constitute grounds for disciplinary action, up to and including termination from employment or other engagement by the Organization, as well as potential civil liability and criminal prosecution.

II. PROCEDURES

1. Any workforce member who believes, in good faith, that he/she or another workforce member has violated any policy and procedure contained in the Organization's HIPAA Compliance Program Manuals, or has inadvertently or purposefully breached the confidentiality of Protected Health Information, MUST report same to the Privacy Officer. If the reporting individual is uncomfortable reporting to the Privacy Officer for any reason, or the Privacy Officer is the perpetrator of the offense, the individual must make the report directly to the Executive Director or through the Organization's Corporate Compliance Line link on the Organization's website, by logging in with your username and password and clicking on the link titled "Corporate Compliance Line."

2. The Organization will not take retaliatory action against any workforce member for the good-faith reporting of HIPAA violations.

3. The Privacy Officer, and where appropriate the Security Officer, will investigate each report in consultation with the Compliance Committee. Workforce members are required to cooperate with the Privacy Officer, Security Officer and other Organization members in any investigation under this Policy.

4. The Privacy Officer, in collaboration with the Human Resources Director, will make a recommendation for action, including sanctions where appropriate, to the Executive Director, who will review the recommendations and make a determination regarding appropriate action, including sanctions where appropriate.

5. Sanctions may include, but not necessarily be limited to, any one or more of the following:

   (a) Re-training.

   (b) Verbal or written warning.

   (c) Verbal or written reprimand.

   (d) Suspension, with or without pay.

   (e) Demotion.

   (f) Removal of right to access Protected Health Information.

   (g) Removal of right to access and utilize electronic systems and devices.

   (h) Imposition of contract penalties.

   (i) Termination.

6. Whether the violation or breach was inadvertent or purposeful, and whether the offender has repeatedly violated or breached, will be taken into consideration in determining sanctions.

7. Where appropriate, and in addition to any other action or sanction, the Privacy Officer will make a report to civil and/or criminal authorities, licensing agencies, accreditation agencies and other appropriate agencies and authorities.

III. REFERENCES

45 C.F.R. § 164.308(a)(1).

EXHIBIT A

HIPAA QUICK REFERENCE GUIDE:
SECURITY RULE STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Administrative Safeguards, 45 C.F.R. § 164.308		
Standard/Safeguard	**C.F.R. Section**	**Implementation Specifications (R) = Required (A) = Addressable**
Security Management Process *(Implement policies and procedures to prevent, detect, contain and correct security violations.)*	164.308(a)(1)	(R) Risk Analysis *(Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the organization.)* (R) Risk Management *(Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to (a) ensure the confidentiality, integrity and availability of all electronic protected health information the organization creates, receives, maintains or transmits; (b) protect against reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures that are not permitted or required under HIPAA; and (d) ensure compliance by the organization's workforce.)* (R) Sanction Policy *(Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the organization.)* (R) Information System Activity Review *(Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking.)*
Assigned Security Responsibility *(Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.)*	164.308(a)(2)	No implementation specification for this standard.

Administrative Safeguards, 45 C.F.R. § 164.308		
Workforce Security *(Implement policies and procedures to ensure that all members of the organization's workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.)*	164.308(a)(3)	(A) Authorization and/or supervision *(Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.)* (A) Workforce Clearance Procedure *(Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.)* (A) Termination Procedures *(Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.)*
Information Access Management *(Implement policies and procedures for authorizing access to electronic protected health information.)*	164.308(a)(4)	(R) Isolating Health Care Clearinghouse Functions *(Only applicable to a health care clearinghouse.)* (A) Access Authorization *(Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction program, process or other mechanism.)* (A) Access Establishment and Modification *(Implement policies and procedures that, based upon the organization's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process.)*
Security Awareness and Training *(Implement a security awareness and training program for all members of the workforce, including management.)*	164.308(a)(5)	(A) Security Reminders *(Periodic security updates.)* (A) Protection from Malicious Software *(Procedures for guarding against, detecting and reporting malicious software.)* (A) Log-In Monitoring *(Procedures for monitoring log-in attempts and reporting discrepancies.)* (A) Password Management *(Procedures for creating, changing and safeguarding passwords.)*

Administrative Safeguards, 45 C.F.R. § 164.308		
Security Incident Procedures *(Implement policies and procedures to address security incidents.)*	164.308(a)(6)	(R) Response and Reporting *(Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the organization; and document security incidents and their outcomes.)*
Contingency Plan *(Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain electronic protected health information.)*	1654.308(a)(7)	(R) Data Back-Up Plan *(Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.)* (R) Disaster Recovery Plan *(Establish (and implement as needed) procedures to restore any loss of data.)* (R) Emergency Mode Operation Plan *(Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.)* (A) Testing and Revision Procedures *(Implement procedures for periodic testing and revision of contingency plans.)* (A) Applications and Data Criticality Analysis *(Assess the relative criticality of specific applications and data in support of other contingency plan components.)*
Evaluation of Security Policies *(Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which the organization's security policies and procedures meet the requirements of the Security Rule.)*	164.308(a)(8)	No implementation specifications for this standard.

Administrative Safeguards, 45 C.F.R. § 164.308		
Business Associate Contracts and Other Arrangement *(A Covered Entity may permit a Business Associate to create, receive, maintain or transmit electronic protected health information on the Covered Entity's behalf only if the Covered Entity obtains satisfactory assurances that the Business Associate will appropriately safeguard the information.)*	164.308(b)(1)	(R) Written contract or other arrangement *(Document the satisfactory assurances required by 164.308(b)(1) or (b)(2) through a written contract or other arrangement between the Covered Entity and Business Associate.)*

Physical Safeguards, 45 C.F.R. § 164.310		
Standard/Safeguard	**C.F.R. Section**	**Implementation Specifications (R) = Required (A) = Addressable**
Facility Access Controls *(Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.)*	164.310(a)(1)	(A) Contingency Operations *(Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.)* (A) Facility Security Plan *(Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.)* (A) Access Control and Validation Procedures *(Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.)* (A) Maintenance Records *(Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks).)*
Workstation Use *(Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access e-PHI.)*	164.310(b)	No implementation specifications for this standard.
Workstation Security *(Implement physical safeguards for all workstations that access e-PHI, to restrict access to authorized users.)*	164.310(c)	No implementation specifications for this standard.

Physical Safeguards, 45 C.F.R. § 164.310		
Device and Media Controls *(Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain e-PHI into and out of a facility, and the movement of these items within the facility.)*	164.310(d)(1)	(R) Disposal *(Implement policies and procedures to address the final disposition of e-PHI information, and/or the hardware or electronic media on which it is stored.)* (R) Media Re-Use *(Implement procedures for removal of e-PHI from electronic media before the media are made available for re-use.)* (A) Accountability *(Maintain a record of the movements of hardware and electronic media and any person responsible therefore.)* (A) Data Backup and Storage *(Create a retrievable, exact copy of e-PHI, when needed, before movement of equipment.)*

Technical Safeguards, 45 C.F.R. § 164.312		
Standard/Safeguard	**C.F.R. Section**	**Implementation Specifications (R) = Required (A) = Addressable**
Access Control *(Implement technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).)*	164.312(a)(1)	(R) Unique User Identification *(Assign a unique name and/or number for identifying and tracking user identity.)* (R) Emergency Access Procedure *(Establish (and implement as needed) procedures for obtaining necessary e-PHI during an emergency.)* (A) Automatic Logoff *(Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.)* (A) Encryption and Decryption *(Implement a mechanism to encrypt and decrypt e-PHI.)*
Audit Controls *(Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.)*	164.312(b)	No implementation specifications for this standard.
Integrity *(Implement policies and procedures to protect e-PHI from improper alteration or destruction.)*	164.312(c)(1)	(A) Mechanisms to Authenticate e-PHI *(Implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner.)*
Person or Entity Authentication *(Implement procedures to verify that a person or entity seeking access to e-PHI is the one claimed.)*	164.312(d)	No implementation specifications for this standard.

Technical Safeguards, 45 C.F.R. § 164.312		
Transmission Security *(Implement technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network.)*	164.312(e)(1)	(A) Integrity Controls *(Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until disposed of.)* (A) Encryption *(Implement a mechanism to encrypt e-PHI whenever deemed appropriate.)*

EXHIBIT B

SECURITY RISK ANALYSIS GUIDANCE AND RISK ASSESSMENT TOOL

Guidance Resources:

HHS.gov guidance on risk analysis, found at:

https://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

NIST Resource Guide for Implementing the HIPAA Security Rule, Special Publication 800-66 Revision 1, found at:

http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

HealthIT.gov Security Risk Assessment Tool:

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

RISK ANALYSIS TABLES

LIKELIHOOD OF OCCURRENCE LEVELS

Likelihood	***Description***
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur once every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month.
Extreme	Likely to occur multiple times per day.

IMPACT SEVERITY LEVELS

Impact Severity	***Description***
Insignificant	Will have almost no impact if threat is realized.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of significant information or services.
Critical	May cause system extended outage or to be permanently closed. May result in complete compromise of information or services

RISK LEVELS

RISK LEVELS	***IMPACT SEVERITY***					
Likelihood of Occurrence	***Insignificant***	***Minor***	***Significant***	***Damaging***	***Serious***	***Critical***
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

EXHIBIT C

DATA BACK-UP PLAN

[*Attached*.]

EXHIBIT D

DISASTER RECOVERY PLAN

[*Attached*.]

EXHIBIT E

EMERGENCY MODE OPERATION PLAN

[*Attached*.]