Credo Health, Inc.

Business Associate HIPAA Security Policy and Procedures Manual

May 13, 2022

TABLE OF CONTENTS

1.0 INTRODUCTION

1.01 Introduction

The Health Insurance Portability and Accountability Act of 1996, including its regulations implementing certain privacy requirements (the "Privacy Rule"), certain breach notification requirements (the "Breach Notification Rule"), and certain security requirements regarding information transmitted by or maintained in Electronic Media (the "Security Rule"), each as amended from time to time (collectively "HIPAA"), and as enforced by the US Department of Health and Human Services ("HHS"), imposes certain health information obligations on Credo Health, Inc. (the "Company") acting in its capacity as a Business Associate to Covered Entities. These obligations concern the privacy and security of individually identifiable health information that the Company receives from Covered Entities or creates, maintains or transmits on behalf of Covered Entities.

This HIPAA Security Policy and Procedures Manual (the "Policy") describes the policies and procedures of the Company that are intended to comply with the requirements of the Security Rule. The Company's policies and procedures that are intended to comply with the requirements of the Privacy Rule and the Breach Notification Rule are set forth in a separate the Company manual, the "HIPAA Privacy Policy and Procedures Manual."

This Policy contains policies and procedures with respect to Protected Health Information or "PHI," but only PHI that is Electronic Protected Health Information under the Security Rule; which is information transmitted by or maintained in Electronic Media. For purposes of this Policy:

> *Protected Health Information or "PHI"* means information that is individually identifiable health information that would be considered "protected health information" under HIPAA, including information received from a Covered Entity or created, received, or maintained on behalf of a Covered Entity and relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies an individual, or for which there is a reasonable basis to believe the information can be used to identify an individual, including name, date of birth, or social security number. PHI includes information of persons living or who have been deceased for 50 years or less.
>
> *Electronic Media* means media that would be considered "electronic media" under HIPAA, including (1) 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; and (2) 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 paper, via facsimile, and voice via telephone, are not considered to be transmissions via Electronic Media if the information being exchanged did not exist in electronic form immediately before the transmission.

Other words and phrases that are capitalized in this Policy, and not specifically defined when used have special meanings that are defined in Section 8 below; provided that any capitalized term not specifically defined in this Policy shall have the same meaning as is set forth in HIPAA, and all words and phrases defined in Section 8 that are also defined in HIPAA are intended to have the same meaning as is set forth in HIPAA.

The Policy consists of nine (9) sections.

Section 1 is an introduction that describes the purpose of the Policy and its organization.

Section 2 describes the Company's overall policy for protecting PHI.

Section 3 describes the Company's procedures for implementing Administrative Safeguards.

Section 4 describes the Company's procedures for implementing Physical Safeguards.

Section 5 describes the Company's procedures for implementing Technical Safeguards.

Section 6 describes required legal documents including Business Associate Agreements and a description of the Security Rule documentation requirements.

Section 7 describes the Company's policies and procedures for complaints and its prohibition on retaliatory acts.

Section 8 defines key terms that are used in this Policy. The defined terms are capitalized throughout the Policy.

Section 9 contains links to key resources related to the implementation of this Policy, including the text of the HIPAA Security Rule and helpful third-party documents.

It is the Company's policy to comply fully with the Security Rule's requirements. To that end, all members of the Company's workforce who have access to PHI to carry out their duties (the "Workforce") must comply with this Policy. For purposes of this Policy, the Workforce includes individuals who would be considered part of the Company's Workforce under the Privacy Rule, such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company. The Policy (or the applicable portions) will be provided to the Workforce who have Access to PHI. These Workforce members will also receive updates that reflect any changes in law or the Policy's procedures. Workforce members can obtain more information from the Company's Security Official.

No third party rights (including but not limited to rights of the Company, employees, clients, Covered Entities, or Subcontractors) are created by this Policy. The Company reserves the right

to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by the Security Rule, the Policy will be aspirational and will not be binding upon the Company, nor give rise to a violation of the Security Rule. This Policy does not address requirements under other federal laws or under state laws. Furthermore, this Policy is designed solely to meet the Security Rule's requirements and serves no purpose under the Employee Retirement Income Security Act of 1974 ("ERISA"). Thus, this Policy shall not be deemed to constitute a contract under any applicable law, is not a health plan document under ERISA, and individuals may not bring a private cause of action based on this Policy or the Company's obligations under the Security Rule.

2.0 STATEMENT OF SECURITY POLICY

2.01 Statement of Security Policy

The Company will secure electronic health information (known as PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is the Company's policy to:

- Ensure the Confidentiality, Integrity, and Availability of the Company's PHI;
- Protect against any reasonably anticipated Threats or hazards to the security or Integrity of the PHI;
- Protect against any reasonably anticipated uses or Disclosures that are not permitted by the HIPAA Privacy Rule; and
- Ensure Workforce compliance.

The Company will maintain a security infrastructure containing Administrative, Physical, and Technical Safeguards for PHI.

When PHI is shared with a Subcontractor providing services to the Company, the Company will obtain satisfactory assurances from the Subcontractor that it will appropriately safeguard PHI it creates, receives, maintains, or transmits on the Company's behalf.

3.0 ADMINISTRATIVE SAFEGUARDS

3.01 Overview

The Company maintains procedures to manage risks to its PHI, to control Access to its PHI, to train Workforce members regarding PHI protections, to resolve security incidents that may be a Threat to its PHI, and to protect PHI during emergency situations. The Administrative Safeguards include the following sections of this Policy:

Section 3.02 - Security Management Process
The Company will maintain procedures to prevent, detect, and correct security violations. This process will include a risk analysis, ongoing risk management, enforcement of a sanction policy, and review of Information System activity.

Section 3.03 - Assigned Security Responsibility
The Company will designate a single individual who has overall responsibility for the development and implementation of the Policies and Procedures required by the Security Rule and this Policy for the security of its PHI.

Section 3.04 - Workforce Security
The Company will maintain Workforce security measures to assure that all Workforce members with Access to PHI have the appropriate Access authority and clearances, and to prevent Access by those who do not.

Section 3.05 - Information Access Management
The Company will define Access control for all Workforce members authorized to Access PHI and maintain procedures for granting and modifying Access.

Section 3.06 - Security Awareness and Training
The Company will maintain a security awareness and training program for all Workforce members with Access to PHI.

Section 3.07 - Security Incident Procedures
The Company will maintain procedures to handle security incidents, including identification and response plans, mitigation of incidents, and documentation of incidents and their outcomes.

Section 3.08 - Contingency Plan
The Company will maintain a contingency plan for responding to emergencies that affect applications and systems containing PHI.

Section 3.09 - Evaluation
The Company will perform periodic technical and non-technical evaluations based on the requirements of the Security Rule, and in response to environmental or operational changes.

3.02 Security Management Process

The Company maintains a security management process to prevent, detect, contain and correct security violations of applications and/or systems that contain PHI.

a. Risk Analysis (Required)

The Company conducts assessments of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of PHI held by the Company periodically, as warranted by changes in environmental, technological, or operational conditions. To appropriately consider the potential vulnerabilities to the Company's PHI, the Company uses the following risk analysis strategy:

- Identify and document all PHI containing systems or applications (repositories);
- Identify the potential Threats or vulnerabilities to each repository;
- Assign a level of risk to each PHI repository; and
- As appropriate, mitigate the risk to each PHI repository.

A PHI repository may be a database, spreadsheet, folder, storage device, document or other form of electronic information. The Company will perform periodic inventories at regular intervals to ensure that the risk analysis is up-to-date and accurate.

b. Risk Management (Required)

The Company manages risks to its PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Company;
- The Company's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and
- The criticality of the PHI potentially affected.

The Company will perform a periodic technical and non-technical evaluation, based on the standards set forth in the Security Rule, to ensure that the Company's Policies and Procedures are updated as warranted by changes in the Company's environmental or operational conditions affecting the security of PHI.

c. Sanction Policy (Required)

Sanctions against Workforce members for failing to comply with the policies and procedures of the Company set forth in this Policy (subject to protections afforded to whistleblowers, and in compliance with applicable anti-retaliation requirements, see Section 3.10, below) will be

imposed in accordance with the Company's discipline policy, as outlined in the Company's Employee Handbook.

During training, Workforce members will be informed that sanctions may be imposed if the policies and procedures of this Policy are violated. Appropriate sanctions will be determined based on the nature of the violation, its severity, and whether it was intentional or unintentional. Such sanctions may include, without limitation, verbal counseling, written warnings, probationary periods and/or termination of employment.

d. Information System Activity Review (Required)

The following procedures are used to review activity in PHI-containing applications and/or systems in order to appropriately limit PHI access to authorized purposes:

- Access to audit logs will be strictly limited to authorized Workforce members;
- Specific activities will be tracked, as described in Audit Controls (Section 5.03), and regularly reviewed for suspicious activity;
- When internal security scans reveal that a computer system or application that contains PHI (or is connected to a PHI repository) may be vulnerable, the person designated in Section 3.07 will contact the Security Official or his/her designee as soon as possible, and provide a description of the vulnerability and a timeline for securing the vulnerability. Timelines will vary depending on the severity; and
- When Auditing tools reveal unusual activity within a computer system or application that contains PHI (or is connected to an PHI repository) the person designated in Section 3.07 will contact the Security Official or his/her designee as soon as possible, and provide a description of the activity and actions taken to mitigate and/or investigate the unusual network activity.

[45 CFR § 164.308(a)(1)]

3.03 Assigned Security Responsibility

The Company assigns the oversight of compliance with the Security Rule to the HIPAA Security Official. If the Company's Security Official is unable to meet the requirements or responsibilities under the Security Rule and set forth below, or is no longer affiliated with the Company, the Company will assign a new Security Official.

The Security Official is:

Name: Carm Huntress

Phone: 1-(800) 604-5613

Mobile: (617) 306-9636

Email: carm@credohealth.com

Security Official Objectives
Establish accountability for security of Protected Health Information (PHI) for the Company in compliance with HIPAA. The Security Official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the Company's policies and procedures covering the security of, and Access to, PHI in compliance with federal and state laws and the Company's information privacy practices.

Security Official Responsibilities

- Accountable for developing and implementing security policies and procedures for the Company for all members of the Workforce that come in contact with PHI.

- Provide development guidance and assist in the identification, implementation, and maintenance of information security policies and procedures in coordination with the Company management.

- Working and coordinating with the Company's Privacy Official.

- Electronic security training and orientation to all Workforce members, contractors, and other appropriate third parties with Access to PHI.

- Mitigate the effects of all Disclosures that are not HIPAA compliant or contrary to the Company's security goals.

- Cooperate with HHS's Office of Civil Rights, other legal entities, and the Company officers in any compliance review or investigations.

- Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the policies and procedures of this Policy, and the requirements of the Security Rule.

- Work with the Company administration to represent the Company's information security interest with external parties (government bodies) who undertake to adopt or amend security legislation, regulation, or standard.

- Initiate, facilitate, and promote activities to foster information security awareness within the Company.

- Conduct continuous risk assessment and analysis. As significant Threats are discovered, management support for additional initiatives and countermeasures will be sought and implemented.

- Conduct related ongoing compliance monitoring activities in coordination with the Company's other compliance and operational assessment functions.

- Responsible for the PHI security infrastructure of the Company.

- Identify key security initiatives and standards, (e.g., virus protection, security monitoring, intrusion detection, local and remote Access control policies, and other technical security services and mechanisms).

- Establish mechanisms to track Access to PHI as required by law to allow qualified individuals to review or receive a report on such activity.

- Review all system-related information security plans throughout the Company's network to ensure alignment between security and privacy practices.

- Maintain current knowledge of technical security services and mechanisms and monitor advancements in information security technologies to ensure organizational adaptation and compliance.

[45 CFR § 164.308(a)(2)]

3.04 Workforce Security

The Company maintains Workforce security procedures to ensure that all the Company Workforce members have appropriate Access to PHI. These procedures also are intended to prevent those Workforce members who do not have appropriate Access to PHI from obtaining such Access.

a. Authorization and/or Supervision (Addressable)

A record of those Workforce members who require Access to PHI and the scope of such Access necessary to perform the Company administrative functions is maintained by the Company IT and Department Managers. Workforce members who do not have Access to PHI but who have a need to review records containing PHI must be supervised in that activity by someone that has such Access and the technical skills to appropriately supervise said Workforce members.

b. Workforce Clearance Procedure (Addressable)

Workforce members that Access PHI are subject to a background check or screening process to ensure that their Access is appropriate. The screening process will include the following checks:

- Criminal History

- Identity Checks (SSN Verification)

- Education and Credential Verification

- Credit Reports

- Employment and Reference Verification

c. Termination Procedures (Addressable)

If a Workforce member who has Access to PHI is terminated or resigns, the former Workforce member's computer accounts will be disabled, including any accounts used for database Access, dial-up, or Internet Access from a remote location.

[45 CFR § 164.308(a)(3)]

3.05 Information Access Management

To ensure that appropriate Access to PHI is consistent with the HIPAA Privacy Rule, the Company actively manages the rights of Workforce members to Access PHI. To the extent that it is reasonable and appropriate, Access to PHI is limited to Workforce members for purposes of administering the Company's business as permitted by the Privacy Rule and consistent with the Company's policies and procedures.

a. Access Authorization (Addressable)

The Company maintains a record of those Workforce members who require Access to PHI and the scope of such Access necessary to perform services for the Company clients. The list is maintained by IT and Department Managers.

b. Access Establishment and Modification (Addressable)

The Company will review who has Access to PHI and whether such Access is limited to PHI that is minimally necessary to perform the Company administrative functions. The PHI Access Control Checklist is reviewed by IT and Department Managers on a semi-annual interval.

[45 CFR § 164.308(a)(4)]

3.06 Security Awareness And Training

The Company maintains security awareness and training for all Workforce members with Access to any PHI repository. Workforce members will review the Company's HIPAA Security Policy, as appropriate, prior to receiving Access to any PHI, and when changes to Policy's policies and procedures occur that are relevant to their job function.

a. Security Reminders (Addressable)

The Company will provide Workforce members with periodic security updates.

b. Protection from Malicious Software (Addressable)

The Company uses hardware and anti-virus software that scans email attachments and other downloadable files. Every Workstation will have anti-virus software installed and activated. Virus signature files will be routinely updated. Workforce members will be instructed not to open emails unless the message was expected in the course of business or was sent by a source known to the recipient.

c. Log-In Monitoring (Addressable)

The Company maintains procedures for monitoring log-in attempts and reporting discrepancies. For systems containing PHI, logs that track successful logins will be periodically reviewed.

For systems containing PHI, logs that track failed login attempts will be periodically reviewed.

Suspicious login activity will be reported and resolved in accordance with the Company's Security Incident Procedures (Section 3.07).

d. Password Management (Addressable)

Workforce members with Access to the Company's PHI will comply with the Company's password management policy in the Employee Handbook.

[45 CFR § 164.308(a)(5)]

3.07 Security Incident Procedures

The Company maintains procedures addressing Security Incidents that permit the Company to identify and respond to suspected or known Security Incidents, mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Company, and document Security Incidents and their outcomes.

The user of any information technology device connected to or housing PHI will report any suspected or known Security Incident promptly as follows:

For Physical and Technical Security issues:

Name: Carm Huntress

Phone: 1-(800) 604-5613

Mobile: (617) 306-9636

Email: carm@credohealth.com

The above-named contact person will log all pertinent information regarding a security incident including date, time, people contacted, and PHI applications or repositories affected. A written log will be kept for all Security Incidents. The Privacy Official and the Security Official will promptly notify each other (or his or her designee) in the event of any such reports, and cooperate to address and resolve all such issues in compliance with HIPAA. This shall include, without limitation, that the Privacy Official and the Security Official will promptly notify each other (or his or her designee) in the event of Security Incidents that have compromised PHI which cannot be timely restored from backups or other circumstances where the Company's reliance on the Integrity and Availability of PHI is materially affected.

The Security Official and the Privacy Official shall cooperate to mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Company, and document Security Incidents and their outcomes, and as appropriate if the Security Incident constitutes a

reportable data breach in violation of HIPAA Privacy Rules, and in accordance with HIPAA Breach Notification rules.

With respect to each reported incident, the Security Official will ensure that the following actions occur:

- Assess the severity of the compromise
- If feasible, make a backup of the infected system(s) or application(s) to prevent attacker from removing evidence of his or her activities
- If feasible, determine if the hacker has left any programs or files on the infected system(s)
- Check all logs for any suspicious activity.

[45 CFR § 164.308(a)(6)]

3.08 Contingency Plan

The Company maintains a contingency plan that includes procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems and/or applications containing PHI.

a. Data Backup Plan (Required)

The extent to which a backup plan is needed will be determined by the Company's periodic risk analyses, including categories of PHI that require an exact retrievable copy. Those categories of PHI where regular backups are not maintained are not needed for the Company's continued operation.

b. Disaster Recovery Plan (Required)

The Company will restore lost, damaged or destroyed PHI from regularly maintained backups, or other outside sources (e.g., third-party vendors).

c. Emergency Mode Operation Plan (Required)

The Company will permit Access control overrides during emergency situations. In addition, to the extent feasible, the following measures are continued during an emergency:

- Guards
- Lighting
- Locks

d. Testing and Revision Procedures (Addressable)

The contingency plan policies and procedures are tested, reviewed and revised as needed, and if necessary, take reasonable steps to ensure that the policies and procedures are up-to-date and effective. In addition, the Company's Business Continuity Plan (BCP) is updated annually and parts of the plan are tested at least annually.

e. Applications and Data Criticality Analysis (Addressable)

See Risk Management (Section 3.02(b)) for the Company's Applications and Data Criticality Analysis procedure.

[45 CFR § 164.308(a)(7)]

3.09 Evaluation

See Risk Management (Section 3.02(b)) for the Company's Evaluation procedure.

[45 CFR § 164.308(a)(8)]

4.0 PHYSICAL SAFEGUARDS

4.01 Overview

The Company maintains procedures to protect applications, systems and related facilities and equipment housing PHI from natural and environmental hazards, unauthorized intrusion, and other Threats. Physical Safeguards include the following sections of this Policy:

Section 4.02 - Facility Access Controls
The Company will limit physical Access to electronic Information Systems and the facilities in which they are housed, while ensuring that properly authorized Access is allowed.

Section 4.03 - Workstation Use
The Company will specify the proper Workstation functions to be performed, the manner in which those functions are to be performed, and the characteristics of the physical surroundings of Workstations that can Access PHI.

Section 4.04 - Workstation Security
The Company will restrict right of entry to all Workstations that can Access PHI to authorized users.

Section 4.05 - Device and Media Controls
The Company will govern the receipt and removal of hardware and Electronic Media that contain PHI into and out of a Facility, and the movement of these items within the Facility. The security procedure address: (a) the final disposition of PHI and/or the hardware or Electronic Media on which it is stored; (b) the removal of PHI from Electronic Media before the media are made available for re-use; and (c) the creation of retrievable, exact copies of PHI when needed, before movement of equipment occurs. The Security Official will assure that appropriate documentation is maintained to record the movement of hardware and Electronic Media and any person responsible therefor.

4.02 Facility Access Controls

The Company will maintain Facility Access control procedures to limit physical Access to its PHI containing Information Systems and the Facility (or facilities) where they are housed, while ensuring that properly authorized Access is permitted.

a. Contingency Operations (Addressable)

When reasonable and practical, Workforce members and emergency personnel will be given Access to the Company to assist in the restoration of lost data. For additional related procedures see: Data Backup Plan (Section 3.08(a)), Disaster Recovery Plan (Section 3.08 (b)), and Emergency Mode Operation Plan (Section 3.08 (c)). In addition, the following Physical Safeguards will be implemented to support Contingency Operations:

- Fire Detectors: Heat-sensing

- Fire Detectors: Flame-actuated
- Automatic Dial-up Alarm
- Fire Extinguishing Systems: Wet Pipe
- Fire Extinguishing Systems: Dry Pipe

b. Facility Security (Addressable)

The Company will safeguard its equipment from unauthorized physical Access, tampering and theft. The following Physical Safeguards will be implemented to support Facility perimeter security:

- Guards (only on during business hours)
- Lighting
- Physical Locks

In addition, the following Physical Safeguards will be implemented to detect unauthorized intrusions to the Company Facilities:

- Alarms
- Motion Detectors

c. Access Control and Validation Procedures (Addressable)

The Company will control and validate a person's Access to the Company facilities using the following physical Access controls:

- Access control (e.g., key locked system).
- Visitors, upon arrival, must sign-in.
- Visitors must be in the company of a Company Workforce member at all times when they are in an area where PHI is located.

d. Maintenance Records (Addressable)

The Company will maintain a log of repairs and modifications to all physical security safeguards including hardware, locks, doors, and walls.

[45 CFR § 164.310(a)(2)]

4.03 Workstation Use

Workforce members will limit their Access and use of PHI- containing systems, applications, and/or Workstations in accordance with applicable Access control lists. In addition, Workforce members will be prohibited from attempting to bypass security protections and must follow all relevant security measures including: Workstation Security (Section 4.04), Facility Access Controls (Section 4.02), Authorization and/or Supervision (Section 3.04(a)), Access Control (Section 5.02), Audit Controls (Section 5.03), Person or Entity Authentication (Section 5.05), and Transmission Security (Section 5.06).

[45 CFR § 164.310(b)]

4.04 Workstation Security

The Company will impose security procedures for all Workstations that have Access to PHI-containing systems or applications. See also Facility Access Controls (Section 4.02).

[45 CFR § 164.310(c)]

4.05 Device And Media Controls

The Company maintains the following procedures governing the receipt and removal of hardware and Electronic Media that contain PHI, into and out of a Facility, and the movement of these items within the Facility:

The Company will label Electronic Media containing PHI. Each device will have a number that corresponds to a technology asset tracker. This label will identify the device as containing PHI.

a. Disposal and Media Re-Use (Required)

The Company will ensure proper sanitation of all Electronic Media containing PHI before it is transferred from the custody of its current custodian. The proper sanitization method depends on the type of media and the intended disposition of the media.

The Company will not use 'clearing data' as a method for sanitizing media containing PHI. Clearing data (such as formatting or deleting information) removes information from storage media so that the information is unreadable. However, special utility software or techniques can be used to recover the cleared data.

The Company will use the following method for sanitizing Electronic Media containing PHI: Overwriting disk drives, Low-Level formatting and "Zeroing out the drive." CDs are shredded and destroyed.

The Company will require vendors repairing or recovering data from any hard drive containing PHI to sign Business Associate Agreements. Once PHI is recovered or the hard drive is repaired, the original hard drive must be returned to the owner so that the owner can properly dispose of the hard drive.

b. Accountability (Addressable)

The Company will maintain a record of the movements of hardware and electronic media and any person responsible therefor.

c. Data Backup and Storage (Addressable)

As needed, the Company will create a retrievable, exact copy of the PHI (e.g., using a tape back-up, imaging the hard drive, or copying the PHI onto a network hard drive) to assure proper backup and storage.

[45 CFR § 164.310(d)]

5.0 TECHNICAL SAFEGUARDS

5.01 Overview

The Company maintains technology procedures to protect and control Access to PHI. They are designed to guard against unauthorized Access to or alteration of PHI that is stored in an application or system or that is transmitted over a communications network. The Technical Safeguards include the following sections of this Policy.

Section 5.02 - Access Control
The Company will maintain procedures to grant and allow Access to Electronic Information Systems that contain PHI to only those persons or software programs that have appropriate Access rights.

Section 5.03 - Audit Controls
The Company will maintain procedural mechanisms and processes that record and examine activity in Information Systems that contain or use PHI.

Section 5.04 - Integrity
The Company will maintain procedures to protect PHI from improper or unauthorized alteration or destruction.

Section 5.05 - Person or Entity Authentication
The Company will verify that a person or entity seeking Access to PHI is the one claimed.

Section 5.06 - Transmission Security
The Company will guard against unauthorized Access to PHI that is being transmitted over an electronic communications network.

5.02 Access Control

The Company will restrict Access to applications or systems that contain PHI to those users that require Access to PHI to carry out the Company's administrative functions by the following administrative policies and procedures: Sanction Policy (Section 3.02(c)), Information System Activity Review (Section 3.02(d)), Authorization and/or Supervision (Section 3.04(a)), Termination Procedures (Section 3.04(c)), and Information Access Management (Section 3.05).

Access to electronic information systems that contain PHI are also restricted based on the user's identity, and often also restricted based on the user's role.

a. Unique User Identification (Required)

The Company will require user Authentication for all Workforce members seeking Access to network applications or systems containing PHI. That Authentication will require a unique identifier (e.g., a log-in user ID) for each user. See also Person or Entity Authentication (Section 5.05). Workforce members are instructed not to allow others to use their unique user ID and password, smart card, or Authentication information. Workforce members will make a

reasonable effort to verify the Authentication of the person or entity receiving PHI prior to transmission.

Anonymous users will not be permitted Access to PHI. All vendor-supplied passwords will be changed when new software or hardware is added to an electronic Information System containing PHI, or when new software or hardware has Access to such a system.

b. Emergency Access Procedure (Required)

The Company will use the following Contingency Plan (Section 3.08) procedures for obtaining necessary PHI during an emergency:

- Data Backup Plan (Section 3.08(a))
- Disaster Recovery Plan (Section 3.08(b))
- Emergency Mode Operation Plan (Section 3.08(c))

c. Automatic Logoff (Addressable)

Workforce members will log off and secure Workstations when not in use.

Facility Access Controls (Section 4.02) addresses additional Physical Safeguards that will be implemented to protect the security of Workstations.

d. Encryption and Decryption (Addressable)

As appropriate and consistent with guidelines established by the Security Official, PHI will be encrypted when stored and decrypted for use via the following methodology:

- AES 256-excryption whenever possible. In cases where encryption is not available (i.e. mobile devices running on the Android operation system), AES 128-bit encryption will be used.

e. Technical Perimeter Control (Addressable)

The following Technical Safeguards will be used to protect PHI - containing systems from unauthorized Access from outside the Company:

- Quarterly Inspection of UTM Firewalls.
- OpenDNS implemented.

The Company will use the following measures to ensure that system perimeter controls have been effectively configured:

- Source - This test measures the use of scanning with specific source ports through the firewall for enumeration.

- Syn Flood - This tests the firewall's ability to manage an ongoing series of SYN packets coming in.

- ACK - This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

- NULL - This test is to discover the firewall's ability to screen enumeration techniques using NULL packets.

- Protocol - This test is to discover the firewall's ability to screen packets of various protocols.

See also Protection from Malicious Software (Section 3.06(b)).

[45 CFR § 164.312(a)(2)]

5.03 Audit Controls

The following Audit controls will be implemented to identify suspect data Access, assess the effectiveness of the Company's security program, and respond to potential weaknesses:

The Company will monitor:

- Successful Logins

- Failed Login Attempts

- File Accessed

- Security Incidents

- Port Scans

To the extent feasible, all applications and systems containing PHI will record user identity, time, date of change and scope of PHI being accessed.

Audit logs will be maintained by the application and/or systems containing or having Access to PHI indefinitely.

See also Information System Activity Review (Section 3.02(d)), Log-in Monitoring (Section 3.06(c)) and Security Incident Procedures (Section 3.07).

[45 CFR § 164.312(b)]

5.04 Integrity

The Company maintains procedures to authenticate PHI and to protect PHI from improper alteration or destruction.

To the extent feasible, the Company will verify that PHI contained within all applications and systems has not been altered or destroyed in an unauthorized manner by using the following electronic mechanisms:

- Checksums (Checksums belong to a class of hashing algorithms designed to detect errors or changes to data (e.g. Tripwire)).
- Record Counts.
- Data Edit Routines.
- Parity Memory (The most common type of memory found on servers and workstations).
- SAN Storage replication and Data Backup System replication
- Uninterruptible Power Supply (UPS).

[45 CFR § 164.312(c)]

5.05 Person or Entity Authentication

The Company will require specific ID and Password authentication to verify user identity of persons Accessing PHI-containing applications/or systems.

[45 CFR § 164.312(d)]

5.06 Transmission Security

The Company maintains transmission security procedures to guard against unauthorized Access to PHI that is being transmitted over an electronic communications network.

The Company will use at least one of the following methodologies to secure PHI when it is being transmitted over an open electronic network:

- WPA-2 wireless network that is approved by the Security Official
- Mobile hotspots that are owned by the Company and have been approved for use to access PHI

Remote computer Access to PHI will only be provided to personnel who have demonstrated a need to Access PHI from off-site locations. (Authorization by the CEO)

The Company will require users seeking remote Access to PHI containing systems or applications to use the following safeguards:

- WPA-2 wireless network that is approved by the Security Official

- Mobile hotspots that are owned by the Company and have been approved for use to access PHI

a. Integrity Controls (Addressable)

In addition to the above under Section 5.06, see Mechanism to Authenticate PHI (Section 5.04) for the Company's integrity controls procedure.

b. Encryption (Addressable)

See above Section 5.06 for the Company's Transmission Encryption procedure.

[45 CFR § 164.312(e)]

6.0 REQUIRED LEGAL DOCUMENTS

6.01 Overview

The Company will enter in a Business Associate Agreement with all Covered Entities. The Company will execute and retain copies of all necessary legal documentation as described in the following sections of this Policy:

Section 6.02 - Business Associate Contracts and Other Arrangements
The Company may permit a Subcontractor to create, receive, maintain, or transmit PHI on its behalf, only if the Company obtains a written contract or other documented arrangement with the Subcontractor as required by HIPAA. The contract or documented arrangement must provide satisfactory assurances that the Subcontractor will appropriately safeguard PHI.

Section 6.03 - Policies and Procedures This Policy is intended to comprise of the policies and procedures to comply with the HIPAA Security Rule, which are reasonably designed and appropriate for the size and type of activities that relate to PHI. Any organizational or technological changes may require updates to this Policy.

Section 6.04 - Documentation
If an action, activity, or assessment is required by the HIPAA Security Rule to be documented, the Company will also maintain a record of that action, activity, or assessment, in accordance with HIPAA requirements.

6.02 Business Associate Contracts and Other Arrangements

The Company will obtain signed Business Associate Agreements that comply with HIPAA from all Subcontractors. In these Business Associate Agreements the Subcontractor must, among other things, agree to comply with the applicable requirements of the Security Rule.

A Subcontractor must sign a Business Associate Agreement. The Company will not disclose PHI to a Subcontractor unless a Business Associate Agreement has been signed.

The Security Official will monitor the PHI that a Subcontractor must return to the Company or destroy (or extend the protections of the Business Associate Agreement if the PHI is not returned or destroyed) upon termination of the Business Associate Agreement.

If the Security Official knows or suspects that a Subcontractor is violating the terms of its Business Associate Agreement, the Security Official will promptly notify the Privacy Official, and the Security Official and Privacy Official will cooperate to determine if a breach has occurred, if the breach can be cured, and to take any other actions that are indicated under HIPAA and otherwise appropriate.

[45 CFR § 164.308(b), 45 CFR § 164.314(a)]

6.03 Policies And Procedures

The Company will implement reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule, and such policies and procedures shall be set forth in this Policy. The Company may change its policies and procedures at any time and shall document such changes in this Policy, in accordance with Section 6.04 of this Policy, and implement such changes in accordance with the Security Rule.

[45 CFR § 164.316(a)]

6.04 Documentation

The Company will comply with the Security Rule requirements regarding documentation creation and retention.

a. Required Versus Addressable

The Security Rule categorizes implementation requirements as either "required" or "addressable." When a standard includes required implementation specifications, the Company shall implement those specifications. When a standard includes addressable implementation specifications, the Company must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, and implement the implementation specification if reasonable and appropriate. If implementing the specification is not reasonable and appropriate, the Company must document why it is not reasonable and appropriate to implement and implement an equivalent alternative measure if reasonable and appropriate.

a. Document Retention

The Company will retain all documentation required by the HIPAA Security Rule for 6 years from the later of the date of its creation or the date when it was last in effect, whichever is later.

b. Availability

The Company will make documentation available to those persons responsible for implementing the procedures, set forth in this Policy, to which the documentation pertains. See also Security Awareness and Training (Section 3.06).

c. Updates

The Company will periodically review HIPAA security documentation, and update the documentation in response to environmental or operational changes affecting the security of the PHI, as needed.

[45 CFR § 164.316(b), 45 CFR § 164.306(d)(3)]

7.0 COMPLAINTS; NON-RETALIATION

7.01 Complaints

The Security Official will be the Company's contact person for receiving and handling complaints about the policies and procedures set forth in this Policy, and the Company's compliance with this Policy or the requirements of the Security Rule, and for handling such complaints. The procedure for doing so shall be the complaints procedure outlined in the HIPAA Privacy Policy and Procedures Manual, which is maintained by the Privacy Official.

The Security Official will document complaints received and their resolutions in accordance with the Policy's documentation procedures at Section 6.04.

7.02 No Intimidating or Retaliatory Acts

The Company, in compliance with HIPAA, shall not and no employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person: (i) for the exercise of any right established, or for participation in any process provided for by the Security Rule, or (ii) for filing a complaint under HIPAA, or (iii) for testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under HIPAA, or (iv) for opposing any act or practice made unlawful by HIPAA, 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 the Privacy Rule. In addition, the Company shall not require individuals to waive their rights under HIPAA to make a complaint to the Secretary of HHS.

If an employee or other person becomes aware of a violation of the foregoing prohibitions against intimidation, retaliation, etc. the employee or other person will promptly (but not later than 24 hours) notify the HIPAA Security Official, who shall cooperate with the HIPAA Privacy Official in resolving the matter in compliance with HIPAA and this Policy.

[45 CFR § 160.310, 45 CFR § 164.316]

8.0 GLOSSARY

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative Safeguards: Administrative actions and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of the Workforce in relation to the protection of that information.

Audit: Safeguards dealing with ensuring activity involving Access to and modification of sensitive or critical files is logged, monitored, and possible security violations investigated.

Authentication: The corroboration that a person is the one claimed.

Availability: The property that data or information is accessible and useable upon demand by an authorized person.

Business Associate: A person or entity that performs a function or activity regulated by HIPAA on behalf of a Covered Entity and involving PHI. Examples of such functions or activities are claims processing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. A Business Associate may be a Covered Entity.

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity: A health plan (including an employer plan, insurer, HMO, and government coverage such as Medicare); a health care provider (such as a doctor, hospital, or pharmacy) that electronically transmits any health information in connection with a transaction for which HHS has established an electronic data interchange standard; and a health care clearinghouse (an entity that translates electronic information between nonstandard and HIPAA standard transactions). The Covered Entities most likely to work with the Company are health insurance plans and carriers and their business associates. HIPAA requires that the Company enter into a written contract (Business Associate Agreement) with a Covered Entity and Subcontractors regarding PHI.

Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Encryption: 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.

Facility: The physical premises and the interior and exterior of a building(s).

HHS: The United States Department of Health and Human Services.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

Physical Safeguards: Physical measures, policies, and procedures to protect electronic Information Systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Subcontractor: A person to whom a Business Associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such Business Associate.

Technical Safeguards: The technology and the policy and procedures for its use that protect PHI and control access to it.

Threat: A potential force or situation that may exploit (accidentally or intentionally) a specific weakness in the safeguards protecting the Company's PHI.

Workforce: Individuals who would be considered part of the Company's workforce under the Privacy Rule, such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company and who have Access to PHI.

Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and Electronic Media stored in its immediate environment.

[45 CFR § 164.304, 45 CFR § 164.103]

9.0 KEY RESOURCES

9.01 HIPAA Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

9.02 Other Resources

a. NIST Special Publication 800-26

https://www.nist.gov/publications/security-self-assessment-guide-information-technology-systems

b. ISO 17799:2005

https://www.iso.org/standard/39612.html

c. ISO/IEC 27001:2013

https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

d. Federal Information Systems Audit Manual (FISCAM)

http://gao.gov/assets/80/77142.pdf

e. Corporate Governance Task Force Report: A Call To Action (April 2004)

https://www.hsdl.org/?view&did=740049

f. Octave Implementation Guide

https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419

g. NIST Special Publication 800-66

https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final