DISCLAIMER

By viewing, accessing and/or using all or any portion of this complimentary informational database and the Materials (hereinafter defined), you agree that you have read, understood and agree to the following terms and conditions on which they are being made available to you by the National Women's Shelter Network ("NWSN"). *If you do not agree with all of the following terms and conditions, then you must not view, access, or use the Materials (hereinafter defined).*

The NWSN is providing the documents, policies, procedures, information, forms and other materials in this database (collectively, "Materials") for your information purposes only and as samples used by other contributors to the NWSN, free of charge. Neither the NWSN nor any provider in the NWSN contributing to the Materials assumes any liability for the Materials and their contents. Provision of the Materials in this database is not intended to be an approval, endorsement or recommendation of any kind on the part of the NWSN or any contributor of all or any part of the Materials. The Materials are not a substitute for professional advice. The Materials are only samples, may be changed and/or updated in the future without notification, and may not be applicable to your or any other person or organization's particular situation. Your use of the Materials is entirely at your own risk, and you should not use the Materials for any purpose without seeking the advice of an attorney licensed to practice in your jurisdiction for your particular circumstances.

Further to that end, the NWSN and all contributors of the Materials assume no responsibility for and make no representations as to the accuracy, usefulness, completeness, legal effect, or suitability of the Materials for any particular purpose. THE MATERIALS ARE PROVIDED "AS-IS" AND "AS AVAILABLE," WITH "ALL FAULTS" and THE NWSN DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, CONCERNING THE MATERIALS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE NWSN FURTHER DISCLAIMS ALL LIABILITY OR RESPONSIBILITY FOR THE CONTENTS OF THE MATERIALS OR OTHERWISE ON THIS WEB PAGE.

Neither the NWSN or any contributor to the Materials is liable for personal injury or damages of any kind arising from the provision or use of all or any part of the Materials, including, but not limited to, whether arising directly or indirectly, death, damage, destruction, personal injury, lost profits, incidental, special or consequential damages. Further, the NWSN shall not be held liable for any use or misuse of the Materials. The posting of the Materials does not imply endorsement, approval, or recommendation.

The information included in this database and the Materials may not be copied, used, disseminated or published in any manner without expressly referencing the foregoing conditions.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

POLICIES AND PROCEDURES MANUAL

Dated As Of October 15, 2010

Revised as of:

December 29, 2011

May 31, 2012

July 24, 2013

October 3, 2014

March 21, 2018

November 2018

June 2019

May 2020

March 2021

February 2022

This HIPAA Policies and Procedures and Risk Management Manual is adopted by [redacted] "Covered Entity") to ensure compliance with the privacy and security rules of the Health Insurance Portability and Accountability Act in furtherance of Covered Entity's mission to provide free shelter and support services to assist indigent and homeless women and children build a safe, secure and better way of life.

The contents of this manual are the confidential and are the proprietary property of the [redacted] The information contained herein may not be copied or used in any way other than the manner in which it is utilized in this manual.

Table of Contents

I. DEFINITIONS

This Manual has been developed by close reference to the *National Institute of Standards Technology Special Publication 800-66 Revision 1, An introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Action (HIPAA) Security Rule* **(NIST 80066)**, available here: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf, a copy of which is appended to this Manual as **Appendix 1**.

To ensure consistency, all capitalized terms used in this Manual not otherwise defined shall have the same meanings as set forth in the NIST 800.

The following definitions are of particular importance and therefore repeated here:

Health Information means: Any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

Individually Identifiable Health Information (IIHI) means: Information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI) means: individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

Electronic Health Information (EPHI) means: information that comes within paragraphs (1)(i) or (1)(ii) of the definition of Protected Health Information.

II. PURPOSE

This Manual is intended to support the compliance efforts of Covered Entity in many ways, including:

- Ensuring that Covered Entity utilizes methods and controls which adequately and appropriately protect EPHI of which they are the steward;
- Establishing compliance strategies that are in concert with the size and structure of the Covered Entities;
- Implementing an ongoing risk management program; and
- Creating appropriate documentation that demonstrates effective compliance with the HIPAA Security Rule.

The HIPAA Security Rule specifically focuses on protecting the safeguarding of EPHI. This Manual is also a vehicle for the Covered Entity to ensure that all Protected Health Information, in addition to EPHI, is properly safeguarded and accorded Confidentiality. Therefore, this Manual includes policies and procedures, as well as specific steps for implementation, that are specific to PHI in addition to EPHI.

III. PRIVACY AND SECURITY POLICIES

A. PRIVACY POLICY

[redacted] It is acknowledged that PHI, EPHI and other information may be created, received, used, released and disclosed in the ordinary course of, and as necessary and appropriate to, providing shelter and rendering services, such as case management, resource coordination and advocacy assistance, to women and children at [redacted], including in many cases making referrals to and assisting in obtaining housing, services, resources and benefits from third parties; *provided however*, any release or disclosure of PHI or EPHI is subject to and in accordance with the consents to release and disclosure signed by the affected women (and in the case of children, their mother). Given the extensive and far-reaching nature of the services provided by Covered Entity at [redacted] it is not possible to delineate all the many consents and releases that are necessary and appropriate in the furtherance of such services, and accordingly standard forms of consents and releases have been created and will be utilized for such purposes. Included in **Appendix 2A** are the standard forms of consents to receive, use, release and disclose PHI and EPHI, as well as other information pertaining to women and children served, in connection with [redacted] Covered Entity may request and respond to other consents to receive, use, release and disclose PHI and EPHI, upon request of the affected women (and in the case of children, their mother), in such other forms as may be requested in addition to the standard forms used.

[redacted] The health care services that may be rendered at the [redacted] are under the auspices of the Department of Health [redacted] and accordingly, Covered Entity shall comply with the privacy rules and practices set forth in the *Notice of Privacy Practices* included in **Appendix 2B**. It is acknowledged that PHI and EPHI may be created, received, used, released and disclosed in the ordinary course of, and as necessary and appropriate to, providing health and wellness services at [redacted] including in many cases making referrals to and assisting in obtaining health services, resources and benefits from third parties; *provided however*, any release or disclosure of PHI or EPHI obtained in connection with the [redacted] is subject to and in accordance with the Notice of Privacy Practices and the consents to release and disclosure signed by the affected women (and in the case of children, their mothers). Included in **Appendix 2A** are various forms of consents to receive, use, release and disclose PHI and EPHI, as well as other information pertaining to women and children served, in connection with the [redacted] Covered Entity may request and respond to other consents to receive, use, release and disclose PHI and EPHI, upon request of the affected women (and in the case of children, their mother), in such other forms as may be requested in addition to the standard forms used.

B. SECURITY POLICY

Covered Entity maintains PHI and EPHI in an electronic health records (EHR) system. This system is maintained in a HIPAA-compliant, cloud-based system, that can only be accessed by designated staff members. The system is password protected. Guest files are created and maintained in this database. The Foundation has a signed HIPAA-compliant Business Associate Agreement with its current EHR software provide [redacted] In addition, the Foundation uses a HIPAA-compliant cloud-based email and document and spreadsheet system with google, password protected pursuant to the Privacy and Security Rule requirements and this manual. The Foundation has a signed HIPAA-compliant Business Associate Agreement with Google for this system. The Foundation also uses a HIPAA-compliant, cloud-based research database [redacted] to maintain data used for research. The Foundation has a signed HIPAA-compliant Business Associate Agreement with [redacted] for this system.

As required by the Security Rule, Covered Entity will utilize the policies and procedures as set forth in this Manual to:

- Ensure the confidentiality, integrity, and availability of PHI and EPHI that it creates, receives, maintains, or transmits;

- Protect against any reasonably anticipated threats and hazards to the security or integrity of PHI and EPHI; and

- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

In complying with this section of the Security Rule, the definitions of § 164.304 are important to understand:

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

Integrity is "the property that data or information have not been altered or destroyed in an unauthorized manner."

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

The policies and procedures in the sections which follow are designed to comply with and carry out the Security Rule and include**: Security Standards – General Rules**, **Administrative Safeguards**, **Physical Safeguards**, **Technical Safeguards**, **Organizational and Documentation Requirements**, and **Documentation**. Within each section are required standards and implementation specifications, which are more detailed methods and approaches Covered Entity has adopted to comply with the standards. In cases where an implementation specification is identified as "addressable" under the Security Rule, Covered Entity has made a

determination of whether it was reasonable and appropriate to implement the specification or provide an equivalent alternative measure that allows it to comply with the standard or alternative measures that are reasonable and appropriate within its environment. This Manual (including Appendices) documents the assessments and decisions made, which are subject to re-evaluation as and when appropriate, but not less than annually, from the date last evaluated.

NOTE, policies and procedures are to be read, insofar as reasonable and appropriate, as supplementing and not in lieu of the policies and procedures required by the [redacted] [redacted] In the event of any inconsistency, [redacted] policies and procedures shall control to ensure compliance with such grant requirements.

III. ORGANIZATIONAL STRATEGIES FOR RISK MANAGEMENT

The assessment, analysis and management of risk provides the foundation of Covered Entity's Security Rule compliance efforts, serving as tools to develop and maintain a strategy to protect the confidentiality, integrity, and availability of EPHI. All EPHI created, received, maintained, or transmitted by a covered entity is subject to the Security Rule and Covered Entity shall implement reasonable and appropriate security measures to protect against reasonably anticipated threats or vulnerabilities to the security of EPHI. This Manual provides a framework for ongoing risk management to effectively manage risks and protect EPHI. Covered Entity has evaluated risks and vulnerabilities in its environment and this Manual sets forth security controls to address those risks and vulnerabilities. The selection and specification of security controls is part of an organization-wide information security program that involves the management of organizational risk – that is, the risk to information, individuals, and the organization as a whole. The management of risk is a key element in Covered Entity's information security program and provides an effective framework for selecting the appropriate security controls for an information system – the security controls necessary to protect individuals and the operations and assets of the organization. This Manual documents the assessments and decisions made as part of the risk management strategy for Covered Entity, which are subject to re-evaluation as and when appropriate, but not less than annually, from the date last evaluated.

The NIST 800-66 includes a helpful tool with six steps for risk evaluation and management which Covered Entity will use as a tool to help in the identification of risks and vulnerabilities, not only in the preparation but continual updating of this Manual to comply with the Security Rule. This section describes a process of managing risk to organizational missions and business functions that arise from the operation and use of information systems by discussing each phase of the NIST Risk Management Framework and providing a mapping of this framework to complementary requirements of the HIPAA Security Rule. The six steps include: 1) Categorize Information Systems, 2) Select Security Controls, 3) Implement Security Controls, 4) Assess Security Controls, 5) Authorized Information Systems, and 6) Monitor Security State. This process will be documented at the outset and at least annually, from the date last evaluated. A copy of the NIST RMF tool along with current assessment is included as **Appendix 3** of this Manual. The steps are intended to provide for critical review and analysis and thoughtful decision-making at each phase, and are ongoing. This risk management process helps to ensure that the procedures and implementation specifications for complying with the standards are continually reviewed and updated, such that this Manual is a living and breathing tool that helps Covered Entity achieve its goal of compliance with HIPAA in furtherance of its overall mission.

It is acknowledged that Covered Entity is a moderately-sized organization that provides free services and operates with a limited budget and modest workforce. It is committed nonetheless to compliance with Security Rule and doing so with reasonable and appropriate means.

IV. ADMINISTRATIVE SAFEGUARDS

A. *SECURITY MANAGEMENT PROCESS*

Covered Entity adopts the following policies and procedures to prevent, detect, contain and correct security violations.

1. Identify Relevant Information Systems, including all information systems that house EPHI, all hardware and software that are used to collect, store, process or transmit EPHI, and analyze business functions and verify ownership and control of information system elements, as necessary. A full and complete inventory of the relevant information systems, hardware, software, business functions, and control of items referenced, which should be updated as appropriate, is included in **Appendix 4**.

2. Conduct periodic Risk Assessment, including an accurate and thorough assessment of the risks and vulnerabilities of the confidentiality, integrity and availability of EPHI held by the Covered Entity, utilizing the risk assessment methodology of NIST SP 800-30, included in **Appendix 5.** A copy of the risk assessment, which should be updated as appropriate, is included in this Appendix. This risk assessment may be updated more frequently where reasonable and appropriate.

3. Implement the Risk Management Program, including security measures to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule, as more fully set forth in the policies and procedures in this Manual and in particular in Section D above. The Program must answer affirmatively the questions:

    - Do current safeguards ensure the confidentiality, integrity and availability of all EPHI?
    - Do current safeguards protect against disclosure other than that permitted or required by the Privacy Rule?"
    - Has the covered entity protected against all reasonably anticipated threats or hazards to the security and integrity of EPHI?
    - Has the covered entity assured compliance with all policies and procedures by its workforce?

4. Acquire IT Systems and Services, as needed to adequately protect information, including additional hardware, software or services, as applicable. Consider in the selection the applicability of the IT solution to Covered Entity's environment, sensitivity of the data, overall security policies and procedures, and other requirements such as resources for operation, maintenance, updating and training.

5. Create and Implement Policies and Procedures Updates, (i) implementing decisions concerning the management, operational and technical controls selected to mitigate risks; (ii) clearly establishing roles and responsibilities and assigning responsibility for implementation to particular individuals; and (iii) procedures and steps to be followed to accomplish security related tasks. Such updates shall be incorporated in this Manual.

6. Implement a Sanction Policy, including appropriate sanctions against workforce members who fail to comply with this Manual and procedures for implementing such sanctions. Such sanctions shall be applied and enforced by the Director and/or Executive Director of the Covered Entity. All workforce members, including employees and volunteers, shall be subject to the Sanction Policy and shall sign acknowledgements, which shall be maintained by the Privacy Officers. Such sanctions shall also be covered by the Employee Manual of Covered Entity, which shall be signed by all workforce members employed by Covered Entity, with copies in their respective personnel files. The forms of Acknowledgement and Agreement are attached in **Appendix 6**. The Privacy Policies are intended to supplement and not replace the confidentiality provisions of employee hire letters and the **Employee Manual**, which is included in **Appendix 10**, and includes detailed policies and procedures in regard to the imposition of sanctions.

7. Develop and Employ the Information System Activity Review Process, including regular review records of information system activity, security incident and audit report forms documenting such processes, and maintain these completed forms to record the results of the review process. Forms for the Security Incident Report and Audit Report are included in **Appendix 7** and **Appendix 8**, respectively. Such forms may be revised and updated on an ongoing basis, as reasonable and appropriate.

8. Standard Operating Procedures shall include: (i) reporting by all work force members, immediately upon gaining knowledge, of suspected or actual compromise of any of the policies and procedures in this Manual, and (ii) ongoing monitoring by the Privacy Team of compliance with the policies and procedures in this Manual. Such monitoring shall be performed by the Privacy Team, under the direction of the Privacy Officers, as often as may be reasonable and appropriate but not less than every six months, from the date last reviewed. A security incident report shall be completed in the case of any suspected or actual compromise of the policies and procedures set forth in this Manual learned in the course of such review or otherwise, in the form of the **Security Incident Report** appended in **Appendix 7**. In the case of a suspected or actual compromise, the Privacy Team shall promptly investigate and prepare a **Security Incident Report** for the review and approval of the Privacy Officers, who shall maintain such reports in the form included in **Appendix 7**. The Privacy Officer shall review the results of the report with the Privacy Team, apply sanctions for violations if any, formulate and implement updated policies and procedures where reasonable and appropriate, and retain the files of all such reports.

9. Implement the Information System Activity Review and Audit Process, including auditing of compliance with the Security Standards – General Rules, Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Document Requirements of this Manual. Such audit reviews shall be performed by the Privacy Team and Privacy Officer, under the direction of the Privacy Officer, as often as may be reasonable and appropriate but not less than annually, from the date last reviewed. An Audit Report shall be completed, in the form appended in **Appendix 8**. The Privacy Team shall submit the Audit Report for the review and approval of the Privacy Officer, who shall maintain such reports. The Privacy Officer shall review the results of the report with the Privacy Team, apply sanctions for violations if any, formulate and implement updated policies and procedures where reasonable and appropriate, and

retain the files of all such reports.

B. ASSIGNED SECURITY RESPONSIBILITY

Covered Entity shall identify the security official who is responsible for the development and implementation of the policies and procedures required for the Covered Entity.

1. The Privacy Officer of Covered Entity is the individual who has final responsibility for security, is able to assess effectively security, and serve as the point of contact for security policy, implementation and monitoring. The Privacy Officer shall: (i) oversee the development and community of security policies and procedures; (ii) is responsible for conducting the risk assessment; (iii) shall handle the results of periodic security evaluations and continuous monitoring; (iv) direct IT security purchasing and investment; (v) ensure that security concerns have been addressed in the system implementation; and (vi) be the person authorized to accept risk from information systems on behalf of the Covered Entity.

2. As of the date of this Manual, Privacy Officers shall be the Director and the Associate General Counsel of the Covered Entity, and this Manual shall document the assigned security duties and responsibilities of the Privacy Officer. Additionally, the Privacy Team shall include the Executive Director, Director, Deputy Directors, Clinical Program Directors, Health and Wellness Director, Operations Director, Program Deputy Director, and such other workforce members as the Privacy Officer may designate from time to time. All members of the work force shall be notified to contact the Privacy Officer and Privacy Team in the event of a security problem.

C. WORKFORCE SECURITY

Covered Entity shall assure that all members of its workforce have appropriate access to PHI and EPHI, as provided in the Information Access Management and the policies and procedures listed below.

1. Implement Procedures for Authorization and Supervision which specify the authorization and supervision of workforce members who work with PHI or EPHI and the locations where such information might be accessed, as more particularly described below. The respective employee hire letters shall specify the supervisors of such workforce members. The respective volunteer agreements of workforce members who are volunteers shall also specify their respective supervisors. The policies and procedures below offer more detail and are in addition to the confidentiality provisions set forth in the respective hire letters and volunteer agreements of workforce members, the Employee Manual, and the **Policies and Procedures Manuals** of Covered Entity, included in **Appendix 11**.

2. Clear Job Descriptions and Responsibilities procedures shall include (i) defining roles and responsibilities for all job functions in the hire letters of employees, (ii) assigning appropriate levels of security oversight, training, and access by the Privacy Officer, in cooperation with the workforce member's supervisor, and (iii) identifying in writing who has the business need – and who has been granted permission – to view, alter,

retrieve, and store PHI and EPHI, and at what times, under what circumstances and for what purposes. Employee hire letters for workforce members hired by the Covered Entity include detailed job descriptions and responsibilities. To the extent this policy requires greater specification, the **Functional HIPAA Organizational Chart** included in **Appendix 9** sets forth the current job functions and need to know and access PHI and EPHI of Covered Entity. All members of the workforce shall be informed of this Functional HIPAA Organizational Chart.

3. Criteria and Procedures for Hiring and Assigning Tasks shall endeavor to ensure (i) staff have the necessary knowledge, skills, abilities and training to fulfill particular roles involving access to and use of sensitive information, and (ii) these requirements are included as part of the personnel hiring and training process. It is acknowledged that Covered Entity seeks to hire individuals who have successfully completed the [redacted] program, inasmuch as they are uniquely qualified to understand and mentor the women and children served by [redacted] and further to fulfill its mission to educate, uplift and empower those who have successfully participated in the [redacted] programming. It should be noted that many grants for homeless services encourage employment opportunities for homeless and formerly homeless individuals. To that end, Covered Entity will emphasize the training component of this procedure to hire and assign tasks described herein.

4. Workforce Clearance Procedures shall include: (i) determining that the access of a workforce member to PHI and EPHI is appropriate, and (ii) appropriate screening of persons who will have access to PHI and EPHI. Nonetheless, it shall not be presumed that a prior record or prior history of substance abuse shall disqualify persons from positions of responsibility for PHI or EPHI, so long as Privacy Officer is satisfied that, based on the candidate's successful accomplishment of the [redacted] program, such candidate is capable of, committed to and educable to perform the duties and responsibilities prescribed herein, and possesses the integrity to carry such duties and responsibilities out with honesty and thoroughness.

5. Termination Procedures for workforce members shall include: (i) terminating access to PHI and EPHI when employment of a workforce member ends, (ii) recovery of access control devices (e.g., badges, keys, access cards, etc.) when employment ends, and (iii) deactivating computer access accounts (e.g., disabling user IDs and passwords) and Electronic Medical Records software access usernames and passwords, if applicable. Termination of workforce members who are employees of Covered Entity and volunteers shall be handled by the Director of Covered Entity and other staff members at the direction of the Director, to address the implementation of these procedures in a manner that is consistent with the smooth transition of such member's responsibilities and the procedures incorporated in the Employee Manual.

D. INFORMATION MANAGEMENT ACCESS

Covered Entity shall authorize access to PHI and EPHI that is consistent with the applicable requirements of the policies and procedures listed below.

1. Covered Entity has determined that no clearinghouse functions exist within its

organization, inasmuch as all services provided are free to the women and children served.

2. Authorized Access to PHI or EPHI policies and procedures will be implemented subject to: (i) the determination of which members shall be granted access to PHI or EPHI on the basis of their respective functions and need to know, (ii) access control methods (e.g., functional role based and security control measures, both technical and non-technical), and (iii) a determination of when, to whom, for what purposes, and under what circumstances PHI or EPHI may be provided to persons or entities external to Covered Entity (e.g., business associates, other service or benefits providers, or women and children seeking access to their own PHI or EPHI). The determination of which members of the workforce shall be granted access to PHI or EPHI is made on the basis of their respective functions and need to know in the furtherance of their duties and responsibilities for Covered Entity and the services provided to women and children served by Covered Entity, per the Functional HIPAA Organizational Chart in **Appendix 9**. PHI and EPHI may be released to persons or entities external to Covered Entity (e.g., business associates, other services or benefits providers, or women and children seeking access to their own PHI or EPHI) by members of the workforce identified by function in the Functional Organizational Chart and subject to compliance with the Privacy Policies set forth in Sections C1 or C2, as applicable above, including receipt of signed consents, authorizations, and releases or if applicable written request by women seeking access to their own PHI or EPHI. Release of information to business associates participating in the provision of services on-site at Covered Entity will also be subject to receipt of a signed Acknowledgment of Privacy Practices, Memorandum of Understanding or other agreement (Confidentiality Agreement) approved by the Privacy Officer, confirming their agreement to treat such information in accordance with the requirements of HIPAA, as applicable, and otherwise in a confidential manner. Such Confidentiality Agreements may be in the form included as **Appendix 6** but are subject to approval by the Privacy Officer in whatever form they take. Security control measures include restricted access to computers and passwords, keys, locking offices, and supervision by workforce members who are entitled to access, to ensure the restrictions are effectively carried out, and are discussed more fully below. All questions should be directed to Privacy Officer, who shall make a final determination of whether or not access to or release and disclosure of PHI or EPHI is appropriate under the Privacy and Security Policies and other policies and procedures of this Manual, the other policies, procedures, agreements, and organizational documents of the Covered Entity and applicable law, in her good faith judgment.

3. Access Establishment and Modification policies and procedures will be implemented based upon the Covered Entity authorization policies and establish, document, review, and modify as appropriate a user's right of access to a workstation, transaction, program or process. Refer to the Functional HIPAA Organizational Chart for determining permitted authorization to access, receive, create, use, release, and disclose PHI or EPHI, in accordance with the policies and procedures of this Manual. All members of the workforce should endeavor, to the extent reasonable and appropriate, to release PHI and EPHI on a need to know basis in the furtherance of the services provided on behalf women and children, and in the event of any

questions as to the reasonableness or appropriateness of such release or disclosure, the matter shall be referred to the Privacy Officer for consultation and a final determination. Access to work stations of members of the workforce entitled to access PHI or EPHI shall be limited to the respective member and her/his/their supervisors, through closing or covering from view documents that contain EPHI, restricted access to user passwords and automatic password protected screen savers that operate within 3 minutes or less to obscure content. Members who step away from their workstations for more than 25 minutes are required to log off their computers or adjust their settings so that the computers automatically log off. Each member of the workforce shall take reasonable and appropriate steps to secure PHI and EPHI from the view of others at all times, which may require repositioning the work station to restrict the views of others.

4. Remote access to PHI and EPHI shall not be allowed, without the express prior consent of Privacy Officer and her/his/their determination that adequate security controls are in place. This includes remote access to PHI/EPHI using any software, cloud program, or other secure program through which Electronic Medical Records may be accessed. The staff member assigned by the Privacy Officer will monitor all recorded access to the Electronic Medical Records software, cloud program, or other secure program periodically if the program has this capability. The staff member reviewing this access will alert the Privacy Officer immediately upon any suspicious, unauthorized, or otherwise apparently inappropriate or irregular access to the Electronic Medical Records program, to be addressed by the Privacy Officer.

5. Existing Security Measures Related to Access Controls shall be evaluated on an ongoing basis, including security features already in place as well as those planned for implementation to determine appropriateness, to determine alignment with other existing organizational goals, policies and procedures and agreements, including the Employee Manual and Policies and Procedures Manuals, audit trails, physical access controls and identification and authentication of users.

E. SECURITY AWARENESS AND TRAINING

Covered Entity shall implement a security awareness and training program for all members of its workforce, including management.

1. Though there is a high level of sensitivity to the need for confidentiality, Covered Entity has determined that enhanced awareness, training and education is needed and beneficial for all members of the workforce on an ongoing basis.

2. Covered Entity will carry out at least annual internal training sessions for all employees covering in detail the policies and procedures required by HIPAA and this Manual. Supplemental trainings may be required for updates to the Manual following security incidents and/or audits. All such trainings shall be conducted by Privacy Officer, assisted by the Privacy Team. Members of the Privacy Team shall further be required to complete education or training programs available on-line or in the community. Privacy Officer shall avail her/his/theirself of continuing education on an annual basis.

3. Although it is the policy of Covered Entity to limit the creation and use of EPHI to the extent reasonable and appropriate, members of the workforce with computerized workstations will be trained regarding procedures for: (i) guarding against, detecting, and reporting malicious software; (ii) monitoring log-in attempts and reporting discrepancies; (iii) creating, changing and safeguarding passwords, and (iv) appropriate and authorized access to Electronic Medical Records software, cloud program, or other secure program if and when paperless system of records and files is adopted, including accessing only those files and records on a need to know basis. Passwords shall not be shared by members of the workforce, provided however, the Privacy Officer shall have a complete list of all computer and/or device access passwords and maintains such list in a secure location. Malicious software detection firewalls will be in place for all computerized workstations, that include features to monitor log-in attempts and report discrepancies. The Privacy Team shall be responsible for ensuring compliance with this procedure and monitoring outcomes.

4. Appropriate Awareness and Training Content, Materials and Methods for workforce members may include: (i) topics selected by the Privacy Officer from this Manual and other HIPAA training materials prepared by third parties, and (ii) on-line or other courses offered in the community, based on the functions of the respective workforce members. The Privacy Officer and Privacy Team will prepare and conduct the trainings for members of the workforce. All members of the workforce shall have access to this Manual, which shall be located in an accessible location in work areas. All workforce members employed by Covered Entity shall be required, as part of their duties, to attend such trainings. Member of the Privacy Team may be required, as part of their duties, to obtain some certifications, as required by the Privacy Officer to evidence their understanding of the materials.

5. Trainings will be implemented and scheduled annually by the Privacy Officer and at other times necessary or appropriate following security incidents and/or audits based on information learned.

6. The Privacy Team shall develop special, periodic reminders for distribution to the workforce members to ensure a high level of awareness of the need to follow these policies and procedures and otherwise ensure the confidentiality, integrity and availability of PHI and EPHI.

7. Covered Entity shall Monitor and Evaluate the Training Plan to ensure that: (i) security awareness and the training are current; (ii) conduct training whenever changes occur in Covered Entity's technology and practices, as appropriate, and (ii) implement corrective actions when problems arise. Privacy Officer and selected members of the Privacy Team shall train new employees on security and for any volunteer workforce members located on site, carefully supervise and train, as necessary or appropriate, on the policies and procedures that relevant to their duties. Third party employee trainings and certifications shall be documented in personnel files.

F. SECURITY INCIDENT PROCEDURES

Covered Entity shall implement policies and procedures to address security incidents, including the following.

1. The Goals of Incident Response shall be to: (i) gain an understanding as to what constitutes a true security incident. Under the HIPAA Security Rule, a security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security Incidents are maintained in one location. Covered Entity is required to be ever vigilant and alert to security risks, physical or technological, that could result in a breach of security. All workforce members shall be responsible for reporting suspected or actual security incidents to the Privacy Officer, who shall in turn conduct with the Privacy Team an investigation, prepare a security incident report, and take appropriate follow-up action, which may include sanctions and additional policies and procedures to anticipate and safeguard against the occurrence of similar security incidents. Privacy Officer may utilize the services of third party technological vendors and may, if necessary or appropriate, report such matters to legal or criminal authorities.

2. Covered Entity acknowledges that its organizational size is modest, but at this time will utilize a "Privacy Team" composed of members designated by Privacy Officer who are in a supervisory role and/or have a technological understanding that may be helpful, to assist with training, monitoring, implementation, audit and raising general awareness of these policies and procedures and the need to safeguard PHI and EPHI. The Privacy Team shall meet with the Privacy Officer quarterly to review any items needed. The Privacy Team shall be responsible for investigating security incidents and conducting the audit, with the review of Privacy Officer.

3. Covered Entity shall implement procedures to respond to and report security incidents, including the following: (i) identify and respond to suspected or known security incidents, (ii) mitigate to the extent practicable, harmful effects of security incidents that are known, and (iii) document security incidents and their outcomes. The Privacy Officer and Privacy Team shall be responsible for carrying out these procedures, and shall document their implementation in the Security Incident Reports. The Privacy Officer shall review the incident response procedures with workforce members whose functions are related to the incident and incident response, solicit suggestions for improvements, and make changes to reflect input as reasonable and appropriate. Follow-up action, such as sanctions and updates to the policies and procedures, shall be taken by the Privacy Officer. Mitigation for affected persons shall be as determined by the Privacy Officer on a case by case basis and documented in the Security Incident Report.

4. Covered Entity will incorporate post-incident analysis into updates and revisions to these policies and procedures. Such analysis will seek to measure the effectiveness and update security incident response procedures to reflect lessons learned and identify actions to take that will improve security controls after a security incident. Lessons learned will also be incorporated in additional training for workforce members as necessary and appropriate.

G. CONTINGENCY PLAN

Covered Entity has established and implemented 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 EPHI.

1. Covered Entity has developed a Disaster and Emergency Preparedness and Continuity of Operations Plan (**Contingency Plan**), included in **Appendix 12,** to anticipate, prepare for and respond to, emergencies and other disaster occurrences, in the context of the organization's overall objectives and service needs to the women and children served. The Contingency Plan shall be reviewed and updated regularly for scope, resource requirements, testing, plan maintenance and backup requirements. Training shall be conducted annually, each spring given the organization's location in Florida, with reviews approximately 48 hours prior to any anticipated significant impending natural disaster. The Privacy Officer with the assistance of the Privacy Team will review and update the Contingency Plan policies and procedures relating to EPHI following any significant occurrence and at least annually from the date thereof.

2. Covered Entity shall conduct an Applications and Data Criticality Analysis, as reasonable and appropriate, in support of the Contingency Plan components as they pertain to EPHI. Such analysis will review (i) the activities and materials involving EPHI that are critical to business operations, (ii) identify critical service or operations and the manual and automated processes, if any, supporting them involving EPHI, (iii) determine the amount of time the organization can tolerate disruptions, material and services (e.g., due to power outages), and establish cost effective strategies for recovering these critical service or processes. The Contingency Plan sets forth those steps deemed reasonable and appropriate in light of that policy to safeguard EPHI under such circumstances.

3. Covered Entity shall identify preventive measures for emergencies and disaster occurrences in the Contingency Plan. The Privacy Officer with the assistance of the Privacy Team will review and update the preventive policies and procedures relating to EPHI following any significant occurrence and at least annually from the date thereof.

4. Recovery Strategies shall be included in the Contingency Plan, including emergency modes of operation, adapted to the organization's operating environment. Covered Entity shall ensure that contractual agreements are in place as needed to assist recovery strategies. The Privacy Officer with the assistance of the Privacy Team will review and update the recovery strategies relating to EPHI following any significant occurrence and at least annually from the date thereof.

5. Data Back Up and a Disaster Recovery Plan shall be included in the Contingency Plan, including procedures to enable continuation of critical business processes for protection of EPHI. The Privacy Officer with the assistance of the Privacy Team will review and update the data back up and disaster recovery plan relating to EPHI following any significant occurrence and at least annually from the date thereof.

6. An Emergency Mode Operation Plan shall be included in the Contingency Plan, including procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode. Emergency mode operation involves only those critical business processes that much occur to protect the security of EPHI during and immediately after a crisis situation. The Privacy Officer with the assistance of the Privacy Team will review and update the emergency mode operations plan procedures relating to EPHI following any significant occurrence and at least annually from the date thereof.

7. Testing, Review and Revision of the Contingency Plan policies and procedures relating to EPHI will be conducted annually, and following each significant disaster occurrence or crisis as reasonable or appropriate. At such time, the Privacy Officer and Privacy Team shall train workforce members on any updates to their defined responsibilities and roles.

H. EVALUATION

Covered Entity shall 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 EPHI, which establishes the extent to which an entity's security policies and procedures meet the requirements described below.

1. Covered Entity has determined, as of the creation of this manual, that internal evaluation is most appropriate and reasonable, given the size, budget and available funding of Covered Entity, the training of the workforce, and the qualifications of the Privacy Officer and Privacy Team. Changes in the foregoing may result in a different determination in the future. Should a different determination be made, Covered Entity may engage external expertise to assist the internal evaluation team where additional skills and expertise is determined to be reasonable and appropriate.

2. Covered Entity shall utilize standards and measurements for reviewing all standards and implementation specifications of the Security Rule, including the annual audit process. The periodic audit shall consider all elements of the HIPAA Security Rule, utilizing the Audit Report to track the management, operational and technical issues evaluated. The Audit Report will take into account Covered Entity's policy to limit the creation of EPHI on a needed basis, and monitor the full range of operations and systems related to EPHI. Third party technical assistance may be employed for portions of the evaluation and measurement.

3. The evaluation performed in the audit will be conducted by the Privacy Team under the direction of the Privacy Officer and reviewed by the Privacy Officer for thoroughness and completeness, as well as any follow-up actions that may be reasonable and appropriate. The Privacy Team will collect and document all needed information, including through interviews, review of computer files, client files, logs and tracking reports. Staff members with knowledge of IT security will be included in the Privacy Team or third parties with such knowledge may be engaged to

participate.

4. Results of the evaluation performed in the annual audit will be thoroughly documented in the Audit Report, including each evaluation finding, remediation option and recommendations, and remediation decisions. Gaps between identified risks and mitigating security controls, if any, and any acceptance of risk, including justifications will be included in the report. Priorities and targets for continuous improvement will be noted as well. The Audit Report will be circulated among the Privacy Team and key staff designated to receive it.

5. Evaluations through the audit process will be repeated periodically, at least annually from the date of the last audit. Additional evaluations may be reasonable and appropriate in response to environmental and operational changes in the organization that affect the security of EPHI (e.g., new technology).

I. BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

Covered Entity may permit a business associate to create, receive, maintain, or transmit EPHI or PHI on the Covered Entity's behalf only if the Covered Entity obtains satisfactory assurances, in accordance with the policies and procedures below, that the business associate will appropriately safeguard the information.

1. Covered Entity shall review its existing and prospective business associates who have or may have access to PHI or EPHI to determine if business associate agreements or other arrangements are required. Such agreements must be written, executed and include sufficient language to protect PHI and EPHI, including a means for termination if PHI or EPHI are not being properly safeguarded. Privacy Officer shall be responsible for such review and determination and take steps to ensure that proper agreements are documented.

2. Written Contracts or Other Arrangements shall include satisfactory assurances that PHI and EPHI will be safeguarded, specifying roles and responsibilities and security controls consistent with such obligations, and requirements that address confidentiality, integrity and availability of PHI and EPHI. Training requirements may be included, if reasonable and appropriate.

3. Covered Entity shall establish clear lines of communication and criteria for performance, conduct periodic reviews to measure contract performance and effectiveness, and terminate the contract if security requirements are not being met.

J. Telehealth

Telehealth is hereinafter defined as the transmission of electronic information and use telecommunications technologies to support and promote remote resource coordination, health care, guest involved [redacted] service related education, and public health administration. Covered Entity staff members may only conduct telehealth meetings in specifically identified authorized circumstances approved in advance by their Clinical Department Director, the Director [redacted], or Associate General Counsel.

Covered Entity staff members may only conduct telehealth meetings in private settings or location, such as in an office space, connecting to a guest who is also in a private setting, such as their room, vehicle, etc. Guests should not receive telehealth services in public or semi-public settings. If the telehealth meeting cannot be provided in a private setting, the Covered Entity staff member should discontinue the telehealth meeting until a proper private setting can be obtained by the Covered Entity staff member and the guest.

V. PHYSICAL SAFEGUARDS

A. FACILITY ACCESS CONTROLS

Covered Entity shall implement policies and procedures to limit physical access to its PHI and EPHI and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

1. Covered Entity has conducted an analysis of existing physical security vulnerabilities, including (i) the existing facilities and identified shortfalls and/or vulnerabilities in current physical security capabilities, (ii) assigned degrees of significance to each vulnerability identified and shall ensure that proper access is allowed, and (iii) determined which portions of the facilities require access controls to safeguard PHI and EPHI, such as data centers, peripheral equipment locations, IT staff offices, and workstation locations. Such analysis shall be periodically reviewed in the course of the audit process at least annually, from the last audit date. Currently, guest and alumni information is stored as EPHI. There is a small amount of old guest files (primarily related to employment and to children) that continue to be maintained in locked cabinets and are immediately shredded after confirming that the file has been properly scanned and uploaded to the guest file. In addition, workstations are positioned in ways to minimize public access and viewing, in such portions of the facilities as are locked when workforce members are unable to supervise and sound machines have been installed in counseling rooms to contain verbal exchange of PHI between counselors and guests when inside counseling rooms. Access to PHI or EPHI shall be limited to workforce members as set forth in the Functional HIPAA Organizational Chart, through restrictions in access to EHR systems or other systems containing EPHI and password protected computer work stations. It is also acknowledged that Covered Entity [redacted] There is a fax machine available to all staff,.
2. Covered Entity shall identify corrective measures and activities necessary to correct deficiencies and ensure that proper access is allowed. Designated workforce members, including Operations Managers and the Privacy Officer, will ensure that repairs, upgrades and/or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed. All workforce members shall be responsible for ensuring that facilities are locked when workforce members are unable to be present in the staff areas where PHI and EPHI are stored. All workforce members shall be trained to be sensitive to the need for locking and

securing workstations, file cabinets and doors and windows of staff areas in the facilities where PHI or EPHI are stored.

3. Covered Entity shall implement policies and procedures to safeguard the facility and equipment therein form unauthorized physical access, tampering and theft, as hereafter provided. The facility is accessible primarily via fob, and in some cases manual key, or when the door is unlocked by the front desk staff. All offices lock and only designated staff members have access to each office. All doors are magnetically locking and all windows are hurricane strength. Only workforce members who have a need to use PHI or EPHI shall have access to the EHR system. An annual inventory of the facility shall be conducted each spring, including all equipment, and regular inspections and needed repairs and upgrades shall be undertaken under the direction of the Privacy Officer.

4. Access Control and Validation Procedures for the facilities shall require all visitors to check in with workforce members, to permit confirmation of the appropriateness of their presence on-site. Workforce members shall be ever vigilant in monitoring visitors and unauthorized visitors shall be excluded from the facilities, requiring in some cases the assistance of law enforcement.

5. Covered Entity has established a Contingency Plan, to which reference is made, including procedures in support of restoration of the facilities and lost data in the event of an emergency.

6. Covered Entity shall maintain maintenance records, which shall be maintained by the Operations Director and periodically reviewed by the Privacy Officer.

B. WORKSTATION SECURITY

Covered Entity shall implement safeguards for all workstations that access EPHI, to restrict access to authorized users.

1. Covered Entity shall identify all methods of physical access to workstations and document the different ways workstations are accessed by employees and nonemployees. Workstations shall be positioned however physically to minimize unauthorized viewing of PHI and EPHI by non-employees; staff working directly with guests will assist in protecting PHI by minimizing presence of third parties at staff desks when discussing personal matters with guests; Counselors will count guests' medications in a counseling room or other closed space away from the view of others and not at counselor desks; counselors and resource coordinators are required to scan and upload guest documents to the EHR system the same day as service and place the paper documents in the locking shred box; operations managers deliver guest mail to each guest floors and resource coordinators collect guest mail and distribute it to their guests; all staff upon leaving their workstations must check for and put away PHI and EPHI before leaving their workstations.

2. Covered Entity shall review and determine which types of access hold the greatest threat to security and take steps to minimize such threats. The Privacy Team and

Privacy Officer shall be responsible for such reviews and protective measures on an ongoing basis. The presence of employees at all times in the staff areas of the facilities minimizes the possibility of inappropriate access to PHI and EPHI through workstations, however staff must be trained to be vigilant in safeguarding PHI and EPHI at all times. Workforce members shall be trained to take steps, such as physically covering PHI or screen saving to cover EPHI, to ensure such information will not be visible to any non-employees.

3. Covered Entity shall identify and implement physical safeguards for workstations and other security measures to minimize the possibility of inappropriate access to workstations. For example, Covered Entity shall provide locked storage for laptops when staff are not at their workstation.

C. DEVICE AND MEDIA CONTROLS

Covered Entity shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of the facilities, and the movement of these items within the facilities.

1. Covered Entity shall implement Methods for Final Disposal of EPHI, to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored. In each case in which EPHI and/or the hardware or electronic media on which it is stored may be considered for disposal, the Privacy Officer must first be consulted for appropriate procedures, to ensure that the EPHI may be properly destroyed and cannot be recreated. This procedure shall apply to all reusable media, such as tapes and CDs, hard drives and file servers, and other hardware. The determination and disposal methods of the hardware, software and data itself shall be documented by the Privacy Team, at the direction of the Privacy Officer.

2. Covered Entity shall implement procedures for removal of EPHI from electronic media before the media is made available for reuse, to ensure that (i) EPHI previously stored on electronic media cannot be accessed or reused, (ii) identify removable media and their use, and (ii) EPHI is removed from reusable media before they are used to record new information. The Privacy Team, under the direction of the Privacy Officer, shall be responsible for coordinating the disposal of data and the reuse of the hardware and software. All workforce members with access to EPHI must be appropriately trained on security and risk to EPHI when reusing software and hardware.

3. Covered Entity shall maintain accountability for the movements of hardware and electronic media and any person responsible therefore, ensuring that: (i) EPHI is not inadvertently released or shared with any unauthorized party, and (ii) the Privacy Team under the direction of the Privacy Officer is responsible for, and records the receipt and removal of, hardware and software with EPHI. Workforce members shall not be allowed to remove electronic media that contain or may be used to access EPHI, unless expressly approved by the Privacy Officer. Records of laptops and ipads shall be maintained by the Director of Operations using an electronic software system designed to track portable hardware such as this.

4. Covered Entity shall implement Data Backup and Storage Procedures, including: creating a retrievable exact copy of EPHI, when needed, before movement of equipment, to ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of EPHI during equipment relocation. To the extent reasonable and appropriate, and in accordance with its Contingency Plan, Covered Entity may maintain offsite backup files.

5. As Covered Entity continues to convert old paper records containing PHI to a cloud-based paperless system, computers and hard drives are designated by the Program Deputy Director and Director of Operations to which paper files, including PHI and EPHI, are scanned and then uploaded into Covered Entity's EHR software. This hardware will be protected by password and other controls outlined in this manual, and will minimize the extent to which EPHI is stored on computer hard drives and accessible outside of the Covered Entity's cloud-based electronic database and records systems.

VI. TECHNICAL SAFEGUARDS

A. ACCESS CONTROL

Covered Entity shall implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those person or software programs that have been granted access rights.

1. Covered Entity shall analyze workloads and operations to identify access needs of all users, considering all applications and systems containing EPHI that should be available only to authorized users and integrate these activities into the access granted and management process. This analysis shall take into account identification of all systems or applications with EPHI and how they are housed, user roles relative to those systems and applications, and data or systems accessed remotely. The Functional HIPAA Organizational Chart in **Appendix 9** sets forth the current analysis of Covered Entity.

2. Covered Entity shall further identify access control capabilities of all information systems with EPHI (e.g., how are systems accessed such as viewing data, modifying data, creating data).

3. All system users shall be assigned a unique identifier, that is a unique name and/or number for identifying and tracking user identity, to (i) ensure that system activity can be traced to a specific user, and (ii) ensure that necessary data is available in the system logs to support audit and other business functions. Identifiers will be selected by the Privacy Officer or a staff member designated by the Privacy Officer, with passwords selected individually.

4. Covered Entity's formal policy for access control included in this section, requires workforce members to preserve the confidentiality of both their identifiers and passwords, provided however Privacy Officer shall have such information for access

as needed. Employees may be subject to reprimand or sanction for failure to comply with these access rules. Audits will allow the Privacy Team and Privacy Officer to determine compliance. Annually, staff will change their computer/device access passwords to minimize the chance of unauthorized access. Semi-Annually (every six (6) months), staff will change with Google account password.

5. Access Control Procedures will use existing hardware/software solutions but will be upgraded as reasonable and appropriate subject to available funding. The access control procedures will be managed by the Privacy Officer, assisted by selected members of the Privacy Team and third party consultants as needed.

6. Covered Entity will review and update user access to: (i) enforce policy and procedures as a matter of ongoing operations, (ii) determine if any changes are needed for access control mechanisms, and (iii) require review and consent of the Privacy Officer for updating access when users require initial access, increased access, and access to new or different systems.

7. Where EPHI must be accessed during emergencies, Privacy Officer with the assistance of Privacy Team shall obtain the available and necessary EPHI from back-up data storage if computerized workstations are not functional, per the Contingency Plan.

8. Automatic Logoff will be utilized, where hardware permits such option, after 25 minutes of inactivity; however, password protected screen savers shall be automatically set to 3 minute intervals of inactivity. Because of the modest quantity of EPHI anticipated and the limited resources of Covered Entity, it has been determined that encryption is not reasonable and appropriate at this time.

9. Covered Entity shall terminate access to EPHI if not longer authorized, such as termination of an employee or change in duties which no longer necessitates access to EPHI. Privacy Officer shall make such determinations, as reasonable and appropriate, and Privacy Team shall under the direction of Privacy Officer implement such decisions.

B. AUDIT CONTROLS

Covered Entity shall implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

1. Covered Entity shall determine the activities that need to be tracked or audited, after analyzing: (i) where EPHI is at risk in the organization, (ii) what systems, applications or processes make data vulnerable to unauthorized or inappropriate tampering, uses or disclosures, (iii) what activities should be monitored (e.g., creation, reading, updating, and/or deleting files or records containing EPHI), and (iv) what audit records should include (e.g., user ID, event type, date, time). This analysis permits a determination of the scope of audit controls that will be necessary in information systems that contain or use EHI based on the Covered Entity's risk assessment and other organizational factors, as well as what data needs to be captured.

2. The tools employed for auditing and reviewing system activity may require changes to and upgrades in the system capabilities. Given the limited resources of the Covered Entity, freeware or system provided monitoring tools are the most likely tools. The analysis of such tools shall be conducted annually by the Privacy Team, with recommendations to the Privacy Officer for a final determination and implementation.

3. The Privacy Team shall conduct its audit review periodically, from the most recent audit, or following a security incident, as reasonable and appropriate. Audits will be documented in the Audit Reports included in **Appendix 8**. Recommendations and actions approved by the Privacy Officer shall be communicated to workforce members as reasonable and appropriate. Reprimands and/or sanctions, up to and including termination as determined by the Privacy Officer, will be imposed for exceptions or violations noted in the audit in accordance with this manual and the Employee Manual. Audit information will be retained in the Covered Entity's electronic corporate records, with other books and records maintained by the Privacy Officer.

4. Standard operating procedures for Covered Entity's Audit Controls include: (i) analysis of activities that need to be tracked and audited, (ii) review of tools employed for auditing and reviewing system activity, (iii) audit review with follow-up based on recommendations, (iv) investigation of exceptions or suspected violations, (v) imposition of reprimands and/or sanctions as determined by the Privacy Officer for misuse, abuse and/or fraudulent activity, and (v) consideration of system upgrades or changes based on audit reviews and investigations. Procedures for reprimand and/or sanctions shall be in accordance with the Employee Manual.

5. The initial audit review shall begin one year following the creation of this Manual, or earlier for purposes of testing these procedures and the systems and applications in use.

C. INTEGRITY

Covered Entity shall implement policies and procedures to protect PHI and EPHI from improper alternation or destruction.

1. Covered Entity shall identify all approved users with the ability to alter or destroy data. The Functional HIPAA Organizational Chart included in **Appendix 9** identifies user functions that may receive, create, use, store, release and disclose PHI and EPHI. Alteration or destruction of data requires the consent of the Privacy Officer, who shall first make a determination that such alteration or destruction is not in contravention of the requirements of HIPAA. Workforce members shall be trained not to alter or destroy PHI or EPHI without the prior consent of the Privacy Officer. The audit trail should be designed to track accesses to EPHI, as reasonable and appropriate.

2. System safeguards and applications that minimize risk of modification of EPHI include: (i) selection of hardware and software and upgrades designed to protect the

integrity of systems and data from hackers, and (ii) procedures upon termination of an employee to terminate access to systems and data, such as changing passwords and authorizations.

3. This Manual sets forth the Integrity Policy of Covered Entity, namely to safeguard the confidentiality, integrity and availability of PHI and EPHI and to protect and preserve PHI and EPHI from improper alteration or destruction. This Manual imposes upon all workforce members the obligation to comply with the policies and procedures set forth in this Manual. Failure to do so in any respect may be cause for reprimand and/or sanction, up to and including termination.

4. Covered Entity shall implement procedures to identify and implement methods to protect PHI and EPHI from modification, as well as tools and techniques to support the assurance of integrity, as set forth in this Manual. The current audit, logging and access control techniques set forth in this Manual may be updated as reasonable and appropriate based on Audit Reports and/or in response to Incident Reports.

5. Covered Entity has chosen an EHR system that minimizes the need for additional electronic mechanisms such as magnetic disk storage and server technology in favor of a secure cloud storage system, which does not require such additional mechanisms. In addition, Covered Entity has adopted a cloud-based system with Google for email and for maintaining corporate files, older guest files, grant spreadsheets and other data that do contain PHI/EPHI, as well as a separate cloud-based system [redacted] for research data entry and analysis. Both systems are maintained in a cloud-based format, password protected pursuant to the Privacy and Security Rule requirements and this manual, and do not require magnetic disk storage, error-correcting memory and the like, by virtue of being cloud-based. The requisite HIPAA-compliant Business Associate Agreements are signed in place with all three software system providers.

6. Monitoring on an annual basis through the audit process will be utilized to assess how the process is working, particularly insofar as the frequency of information integrity problems.

D. PERSON OR ENTITY AUTHENTICATION

Covered Entity shall implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

1. Covered Entity has determined the applicability of authentication to systems and applications. Authentication requires establishing the validity of a transmission source and/or verifying a person's claim that s/he has been authorized for specific access privileges to information and information systems. The principal method currently used by Covered Entity for authentication is individual specific passwords.

2. Covered Entity shall periodically and at least annually from the last audit evaluate the relative advantages and disadvantages of commonly used authentication approaches, e.g., passwords, smart cards, biometric identification such as

fingerprint, and combinations of the foregoing.

3. Based on the analysis of current resources, hardware and software being utilized and technical knowledge of staff, Covered Entity has determined that individual passwords are reasonable and appropriate. In addition access to areas where computerized workstations storing EPHI are located is limited. Covered Entity will conduct periodic trainings and reminders on the importance of individual password usage and privacy.

E. TRANSMISSION SECURITY

Covered Entity shall implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

1. Covered Entity has reviewed existing measures to protect EPHI in transmission. Given that Covered Entity provides free services, it is not reasonably foreseeable that business competitors exist who would profit from modification of EPHI. Sources of unauthorized access that may result in modification of EPHI during transmission may be random hackers or disgruntled employees or women served at the shelter; however such risk is deemed to be low given the relatively low technical expertise of employees and women served.

2. Covered Entity has developed the following security policy and procedures applicable to transmission of EPHI, namely Covered Entity (i) staff with access to EPHI are instructed to carefully check all addresses of electronic mail recipients, and facsimile and mail recipients as well, before sending EPHI and PHI, (ii) whenever possible, electronic transmissions by staff with access to EPHI shall use only first names identifiable by the recipient and shall limit the use of identifying information, and (iii) electronic messages of all staff with access to EPHI shall include the following protective language in the "signature" of the email: *CONFIDENTIALITY NOTICE: This message is intended only for the use of the individual or entity to which it is addressed and is covered by the Electronic Communications Privacy Act, 18 USC §§2510-2521, in addition to other applicable laws and regulations, such as the Health Insurance Portability and Accountability Act of 1966, Public Law 104-191. This message is legally privileged and confidential and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone* [redacted] *and delete the original message, and all copies, from your system. Thank you.*

3. The measures described above are intended to protect EPHI from unauthorized interception and/or modification of EPHI.

F. Destruction of Records

Records will be destroyed in a manner that does not allow for the information to be retrievable, recognizable, reconstructed or practically read. Method of destruction must be appropriate for the medium on which it is stored.

G. Telehealth

Telehealth services may be provided securely through telephone phone calls; direct text messaging; electronic mail through the Covered Entity's HIPAA-compliant cloud-based Google email system only; or video telecommunications technologies, specifically videoconferencing software with "non-public facing" remote communication capabilities. A "non-public facing" remote communication videoconferencing software product is one that, as a default, employs end-to-end encryption; allows only the intended parties to observe or participate in the communication; and supports individual user accounts, logins, and passcodes. In addition, participants using a "non-public facing" remote communication videoconferencing software product should be able to assert some degree of control over particular capabilities, such as enabling or disabling recording capabilities, or enabling or disabling audio and/or video signal transmission.

Covered Entity utilizes only the video telecommunications technology services that have "non-public facing" remote communication product capabilities for telehealth services delivered through video telecommunications. Covered Entity will ensure that video telecommunications technology services vendors are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. The list below includes the vendor(s) that represent that they provide HIPAA-compliant video communication products and that have provided Covered Entity with a HIPAA BAA.

- Doxy.me
- Google G Suite (Hangouts and Meet)

From time to time, as necessary, Covered Entity will evaluate, add, or remove the above listed approved video telecommunication providers/products.

VI. ORGANIZATIONAL REQUIREMENTS

A. BUSINESS ASSOCIATE CONTRACTS OR OTHER ARRANGEMENTS

Covered Entity recognizes that (i) a contract or other arrangement between Covered Entity and its business associates who create, receive, maintain, or transmit EPHI must meet the requirements below, (ii) Covered Entity is not in compliance with its own obligations under HIPAA if it knows of a pattern of an activity or practice of the business associate that constitutes a material breach or violation of such associate's obligations to safeguard EPHI under the contract or other arrangement, unless Covered Entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful (a) terminate the contract or other arrangement if feasible, or (b) if termination is not feasible, report the problem to the Secretary of Health and Human Services.

1. Covered Entity's contracts with business associates who create, receive, maintain or transmit EPHI on its behalf must provide that business associates will implement

administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that the business associate creates, receives, maintains, or transmits on behalf of the Covered Entity. The contract should address the functions related to creating, receiving, maintaining or transmitting EPHI on behalf of Covered Entity. Covered Entity may consider asking the business associate to conduct a risk assessment that addresses administrative, technical, and physical risks, if reasonable and appropriate.

2. Contracts with business associates who create, receive, maintain or transmit EPHI on behalf of Covered Entity must provide that any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it.

3. Contracts must provide that business associates who create, receive, maintain or transmit EPHI on behalf of Covered Entity will report to Covered Entity any security incident of which it becomes aware, and a reporting mechanism, and a process for the business associate to use in the event of a security incident shall be in place, identifying the key business associate staff who will serve as the point of contact.

4. Contracts must provide that business associates who create, receive, maintain or transmit EPHI on behalf of Covered Entity can be terminated by the covered Entity if the Covered Entity determines that the business associate has violated a material term of the contract pertaining to the security of EPHI, including establishing in the agreement the circumstances under which a violation of the agreements relating to the security of EPHI constitutes a material breach of the contract. Covered Entity is required to terminate the contract if the Covered Entity learns that the business associate has violated the contract or materially breached it and it is not possible to take reasonable steps to cure the breach or end the violation, as applicable. If termination of the contract is not feasible, Covered Entity is required to report the problem to the Secretary of Health and Human Services.

5. If the business associate that creates, receives, maintains or transmits EPHI on behalf of Covered Entity is required by law to perform a function or activity on behalf of Covered Entity or to provide a service described by section 45 CFR 160.103 to a Covered Entity, Covered Entity may permit the business associate to create, receive, maintain, or transmit EPHI on its behalf to the extent necessary to comply with the legal mandate without meeting the contractual requirements for termination provided that Covered Entity attempts in good faith to obtain and document satisfactory assurances that the security standards required are met and/or the reasons assurances cannot be obtained. Covered Entity may omit from its other arrangements authorization of the termination of the contract by the Covered Entity if such authorization is inconsistent with the statutory obligations of the Covered Entity or its business associate.

B. POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

Covered Entity recognizes that it is required to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other

requirements of HIPAA, taking into account its unique organizational parameters. Covered Entity may change its policies and procedures at any time in the manner provided below.

1. Covered Entity has created this Manual to document reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Privacy Rule and Security Rule, given the size, complexity, and capabilities, as well as the technical infrastructure, hardware and software security capabilities, of the Covered Entity, and costs of security measures. Covered Entity will periodically reevaluate the policies and procedures to verify that policies and procedures (i) are sufficient to address the standards, implementation specifications and other requirements of the Security Rule, and (ii) accurately reflect the actual activities and practices exhibited by the Covered Entity, its staff, systems and business associates.

2. Covered Entity will update and change its policies and procedures as is reasonable and appropriate, at any time, provided that the changes are documented and implemented in accordance with the requirements of the Privacy Rule and Security Rule. Documentation may be reviewed and updated in response to periodic evaluations at least annually from the last audit, following security incidents and/or after acquisitions of new technology, or changes in activities or procedures. Workforce members shall be appropriately trained in regard to pertinent changes.

C. DOCUMENTATION

Covered Entity will maintain policies and procedures implemented to comply with this section in written form (which may be electronic) and if an action, activity or assessment is required by this section to be documented, maintain a written record (which may be electronic) of the action, activity, or assessment.

1. This Manual documents the decisions of Covered Entity concerning the management, operational, and technical controls selected to mitigate identified risks. The appendices also contain forms for documenting Covered Entity's analysis and decisions. Privacy Officer shall maintain a comprehensive record of all of the foregoing.

2. Covered Entity shall retain documentation of policies, procedures, actions, activities or assessments required by the Security Rule for at least six years form the date of creation or when last in effect, whichever is later. Other data retention policies of Covered Entity shall be aligned with this policy, so that they are at least as long.

3. Documentation required under this section shall be made available to persons responsible for implementing the procedures to which the documentation pertains. The Manual shall be maintained in a readily accessible location for staff. The Privacy Officer shall receive and retain all audit and security incident report forms.

4. Documentation shall be reviewed periodically, and updated as needed, in response to environmental or operational changes affecting the security of PHI and EPHI. During the annual audit process and training sessions, staff will be consulted for

input on policies, procedures, implementation specifications for continued timeliness and updates.

5. Records will be destroyed in a manner that does not allow for the information to be retrievable, recognizable, reconstructed or practically read. Method of destruction must be appropriate for the medium on which it is stored.

DISCLAIMER

By viewing, accessing and/or using all or any portion of this complimentary informational database and the Materials (hereinafter defined), you agree that you have read, understood and agree to the following terms and conditions on which they are being made available to you by the National Women's Shelter Network ("NWSN"). *If you do not agree with all of the following terms and conditions, then you must not view, access, or use the Materials (hereinafter defined).*

The NWSN is providing the documents, policies, procedures, information, forms and other materials in this database (collectively, "Materials") for your information purposes only and as samples used by other contributors to the NWSN, free of charge. Neither the NWSN nor any provider in the NWSN contributing to the Materials assumes any liability for the Materials and their contents. Provision of the Materials in this database is not intended to be an approval, endorsement or recommendation of any kind on the part of the NWSN or any contributor of all or any part of the Materials. The Materials are not a substitute for professional advice. The Materials are only samples, may be changed and/or updated in the future without notification, and may not be applicable to your or any other person or organization's particular situation. Your use of the Materials is entirely at your own risk, and you should not use the Materials for any purpose without seeking the advice of an attorney licensed to practice in your jurisdiction for your particular circumstances.

Further to that end, the NWSN and all contributors of the Materials assume no responsibility for and make no representations as to the accuracy, usefulness, completeness, legal effect, or suitability of the Materials for any particular purpose. THE MATERIALS ARE PROVIDED "AS-IS" AND "AS AVAILABLE," WITH "ALL FAULTS" and THE NWSN DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, CONCERNING THE MATERIALS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE NWSN FURTHER DISCLAIMS ALL LIABILITY OR RESPONSIBILITY FOR THE CONTENTS OF THE MATERIALS OR OTHERWISE ON THIS WEB PAGE.

Neither the NWSN or any contributor to the Materials is liable for personal injury or damages of any kind arising from the provision or use of all or any part of the Materials, including, but not limited to, whether arising directly or indirectly, death, damage, destruction, personal injury, lost profits, incidental, special or consequential damages. Further, the NWSN shall not be held liable for any use or misuse of the Materials. The posting of the Materials does not imply endorsement, approval, or recommendation.

The information included in this database and the Materials may not be copied, used, disseminated or published in any manner without expressly referencing the foregoing conditions.