TotalWellness

HIPAA Compliance

Policies and Procedures Manual

Effective: January 1, 2012
Last Update: March 18, 2016
Last Review: April 3, 2024

Prepared by:
Parsonage Vandenack Williams LLC Attorneys at Law
5332 S. 138th St., Suite 100 | Omaha, NE 68137
Telephone: (402) 504-1300 | Facsimile: (402) 504-1935 | www.pvwlaw.com

1. DEFINED TERMS

Corporation	"Corporation" means Vaccination Services of America, Inc. d/b/a TotalWellness
ePHI	"ePHI" means PHI that is maintained or transmitted in an electronic format.
HIPAA	"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended.
HITECH	"HITECH" or the "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, as amended.
Notice	"Notice" means the Corporation's Notice of Privacy Practices pursuant to the Regulations and these Policies.
PHI	"PHI" means protected health information as defined by the Health Insurance Portability and Accountability Act of 1996, as amended; and the regulations promulgated thereunder, e.g. information: (a) that may identify a patient; (b) that relates to a patent's past, present or future physical or mental health or condition and related health care services; and (c) that was created by or received by the Corporation.
Policies	"Policies" means all of the Corporation's HIPAA Compliance Policies and Procedures contained herein.
Privacy Officer	"Privacy Officer" means the Corporation's Privacy Officer as designated by the Corporation. The Privacy Officer and Security Officer may be the same person. The initial Privacy Officer of the Corporation shall be Kate Adams. The current Privacy Officer is Alan Kohll.
Regulations	"Regulations" means HIPAA, as amended by the HITECH Act, and as further amended; the regulations promulgated thereunder; and any statutes or regulations issued by a state or any of its governmental agencies creating more stringent privacy obligations that those set forth under the federal law and regulations mentioned at the beginning of this sentence.
Security Officer	"Security Officer" means the Corporation's Security Officer as designated by the Corporation. The Security Officer and Privacy officer may be the same person. The initial Security Officer of the Corporation shall be Kate Adams. The current Security Officer is Alan Kohll.

2. NOTICE OF PRIVACY PRACTICES

POLICY: It is the Corporation's policy to provide patients with the Notice no later than upon each patient's first receipt of products or services through the Corporation. Upon any revision to the Notice, it is the Corporation's policy to provide patients with the Corporation's then-current Notice no later than upon each patient's first receipt of services through the Corporation after such amendment or supplement. In addition, the Corporation will post the Notice in a conspicuous location and will make the Notice available to all patients upon request. The Corporation may also post the Notice on its web site if the Corporation maintains a web site that provides information about the Corporation's services.

PURPOSE: The purpose of this policy is to explain: (1) the patient's right to the Notice; (2) the relevant procedures the Corporation will follow when providing the Notice to patients; and (3) the requirements for documentation of and revisions to the Notice.

I. RIGHT TO A NOTICE OF PRIVACY PRACTICES

A. Patient's right to notice. Patients have the right to adequate notice of the uses and disclosures of PHI that the Corporation may make, the patient's rights with respect to PHI, and the Corporation's legal obligations regarding PHI.

B. Basic notice requirements. The Notice will be written in plain language and contain all elements required by the Regulations.

II. PROVIDING THE NOTICE TO PATIENTS

A. General rules. The Corporation will follow these rules for providing a paper copy of the Notice to patients and the public in general.

1. The Corporation will make the Notice available upon request to any person, even if the person is not a current Corporation patient.

2. The Corporation will provide the Notice to each of its patients no later than the date that the Corporation first provides services to the patient including service delivered electronically. In emergency treatment situations, the Notice will be provided as soon after the emergency as is reasonably practicable.

3. The Corporation will have the Notice available at the influenza vaccine and/or other wellness service administration location.

B. Electronic notice. The Corporation will provide the Notice electronically under certain circumstances.

1. If the Corporation maintains a web site that provides information about the Corporation's services, the Corporation will prominently post the Notice on the web site and make the Notice available electronically through the web site.

2. The Corporation may provide the Notice to an individual by email, only if the individual agrees to receive materials from the Corporation electronically and the individual has not withdrawn his/her agreement. If the Corporation knows that the email transmission failed, the Corporation will provide a paper copy of the Notice to the individual.

3. If an individual receives an electronic Notice, he/she still has the right to obtain a paper copy of the Notice from the Corporation upon request.

III. REVISIONS TO THE NOTICE

A. The right to change the Notice. The Corporation reserves the right to change its privacy practices and apply the revisions to PHI previously created or retained, and the Corporation will make a statement to that effect in the Notice.

1. Making material changes to the Notice. The Corporation will promptly revise its Notice whenever there is a material change to the uses or disclosures of PHI, the individuals' rights, the Corporation's legal obligations, or other privacy practices stated in the Notice. Whenever the Notice is revised, the Company will make the Notice available upon request on or after the effective date of the revision, promptly make the Notice available at the Company's influenza vaccine and/or other wellness service administration locations, and post the revised Notice on the Company's web site, if any, as set forth in Section II(B) above. Upon any revision to the Notice, it is the Corporation's policy to provide patients with the Corporation's then-current Notice no later than upon each patient's first receipt of services through the Corporation after such revision. The Corporation will provide the revised Notice to its patients in the same manner as it provided the Notice as set forth in Section 2(II) above. If the Corporation revises the Notice, it is not required to distribute the Notice to all former patients until their next receipt of the Corporation's services.

B. Implementation of revised privacy practices. In general, the Corporation may not implement a material change to any term of the Notice before the effective date of the Notice that reflects the material change.

IV. DOCUMENT RETENTION REQUIREMENTS

The Corporation will retain a copy of each Notice it issues for a period of six years from the date that the Notice was last in effect, or longer if required by the Regulations.

3. ACKNOWLEDGMENT

POLICY: It is the Corporation's policy to make a good faith effort to obtain each patient's written acknowledgment that the patient has received the Notice upon the patient's first receipt of services through the Corporation.

PURPOSE: The purpose of this policy is to explain: (1) when the Corporation is required to obtain an acknowledgment; (2) the relevant procedures the Corporation will follow when obtaining the acknowledgment from patients; and (3) the requirements for documentation of the acknowledgment process.

I. OBTAINING AN ACKNOWLEDGMENT

A. Acknowledgement requirement. The Corporation will make a good faith effort to obtain the patient's written acknowledgment of receipt of the Notice no later than the date of first service delivery. In emergency treatment situations, the Corporation may wait to obtain the acknowledgment until reasonably practicable. If the Notice is delivered electronically as part of first delivery of services, the Corporation's computer system will be capable of capturing the patient's acknowledgment of receipt electronically.

B. Patient's failure to provide acknowledgment. If a patient refuses or otherwise fails to provide an acknowledgment, the Corporation will document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.

C. Single acknowledgment. Only one signed acknowledgment is required per patient. Even if the Notice is revised, the Corporation is not required to ask patients to sign a new acknowledgment, but will keep a log of dates and means by which any revised Notice is provided to patients.

II. RECORD RETENTION REQUIREMENTS

The Corporation will retain copies of any written acknowledgements of receipt of the Notice, or, if not obtained, documentation of its good faith efforts to obtain such written acknowledgment along with copies of its logs of efforts to provide revised Notices to patients. The Corporation will retain this documentation from the date of its creation until six (6) years after the date when it was last in effect, or longer if required by the Regulations.

4. GENERAL USE AND DISCLOSURE

POLICY: The Corporation will use and disclose PHI only as specifically permitted or required by the Regulations and in accordance with these Policies.

PURPOSE: The purpose of this policy is to explain the basic standards that will be met when using and disclosing PHI.

I. INTRODUCTION

A. Basic rule for use and disclosure of PHI. The Corporation will not use or disclose PHI unless permitted or required by the Regulations.

B. Permitted uses and disclosures. The Corporation may use and disclose PHI as follows: to the patient; to carry out treatment, payment or health care operations; pursuant to and in compliance with a valid authorization; pursuant to a verbal agreement from a patient that permits disclosure to persons assisting in the patient's care or payment for the patient's care; and for certain "national priority" purposes such as disclosures required by law. The Corporation may share a patient's PHI with third party "business associates" that perform various activities on the Corporation's behalf. Whenever an arrangement between the Corporation and a business associate involves the use or disclosure of a patient's PHI, the Corporation will have a written contract that contains terms that will protect the privacy of the patient's PHI. The Corporation may use or disclose PHI to provide the patient with information about health-related benefits and services that may be of interest to the patient. The patient may contact the Corporation's Privacy Officer in writing to request that these materials not be sent.

C. Incidental uses and disclosures. The Corporation will apply reasonable safeguards and implement the minimum necessary standard in connection with incidental uses and disclosures that occur as a by-product of a use or disclosure otherwise permitted under the Regulations.

D. Required disclosures. The Corporation will disclose PHI when the patient requests access to information about himself/herself; and when the United States Department of Health and Human Services or its authorized representatives or any similar state agency or its authorized representatives requests information to investigate or determine the Corporation's compliance with the Regulations.

II. MINIMUM NECESSARY

A. The minimum necessary standard. When using or disclosing PHI, and when requesting PHI from another entity, the Corporation will make reasonable efforts to use, disclose or request the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request.

B. Exceptions. The Corporation will not use the minimum necessary standard in connection with the following: uses and disclosures for treatment purposes; disclosures to the patient who is the subject of the information; uses or disclosures made pursuant to an authorization; uses or disclosures made in mandatory or situational fields of a HIPAA transactions standard; disclosures to the United States Department of Health and Human Services when required by that agency for compliance and enforcement purposes; and uses or disclosures that are required by other law.

C. Required policies and procedures for uses of PHI. The Corporation has developed and implemented policies that limit the use of PHI to the minimum PHI reasonably necessary to accomplish the intended purpose of the use or disclosure. The only people who will have access to PHI to carry out his/her duties within the Corporation are the nurses administering vaccinations and physicians supervising them, medical professionals providing wellness services, and customer service and administrative personnel. These people will have access to all categories of PHI necessary to carry out their job functions. No person will have access to PHI until such person has completed the training required under these Policies and has signed an acknowledgement of having received such training and understanding these Policies.

D. Required policies and procedures for disclosures of PHI. For any type of disclosures (other than those set forth in Section II(B) above), the Corporation has developed the following criteria for determining and limiting disclosure to only the minimum amount of PHI necessary to accomplish the purpose of the disclosure: How much PHI will be disclosed? To what extent would the disclosure increase the number of persons with access to the PHI? What is the likelihood of further disclosures? How important is the disclosure? Can substantially the same purpose be achieved using de-identified information? Is there technology available to limit the amount of PHI disclosed? What is the cost, financial or otherwise, of limiting the disclosure?

E. Requests for PHI. The minimum necessary standard applies to situations where the Corporation is requesting an individual's PHI from another entity. For all such requests, the Corporation will consider the following factors when reviewing the requests on an individualized basis: How much PHI will be disclosed? To what extent would the disclosure increase the number of persons with access to the PHI? What is the likelihood of further disclosures? How important is the disclosure? Can

substantially the same purpose be achieved using de-identified information? Is there technology available to limit the amount of PHI disclosed? What is the cost, financial or otherwise, of limiting the disclosure?

F. Reasonable reliance on requested disclosures. The Corporation may rely, if reasonable under the circumstances, on statements by public officials, other covered entities or their business associates that they are requesting the minimum PHI necessary to achieve the stated purpose of the request. The Corporation may also reasonably rely on the statements of its own business associates or professionals within its workforce (such as nurses) that the information requested to provide professional services to the Corporation is the minimum necessary for such purposes.

III. DE-IDENTIFICATION AND LIMITED DATA SETS

A. Basic standard. Health information is considered de-identified (*i.e.*, not individually identifiable) if it does not identify a patient and the Corporation has no reasonable basis to believe it can be used to identify a patient. Health information that is de-identified pursuant to the Regulations is not PHI and therefore HIPAA requirements do not apply to such information.

B. De-identifying information. The Corporation may de-identify information in two ways: if a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination on the basis of the Regulations, and documents the analysis, that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information; or if pursuant to the Regulations the Corporation removes a list of specified identifying information about the individual or his/her relatives, employers, or household members, and the Corporation has no actual knowledge that the information could be used alone or in combination to identify a subject of the information.

C. Use of PHI to create de-identified information. The Corporation may use PHI to create de-identified information, or may disclose PHI to a business associate for such purpose, whether or not the de-identified information will be used by the Corporation.

D. Re-identification. If de-identified information is re-identified at some point by the Corporation, it becomes PHI again for all purposes and therefore subject to these Policies and the Regulations.

E. Limited data set. The Corporation may use PHI, or disclose PHI to a business associate, for the creation of a limited data set. A limited data set may be used or disclosed only for the purposes of research, public health, or health care operations, so long as the Corporation enters into a data use agreement with the recipient of the limited data set.

1. A limited data set is PHI that excludes specified direct or "facial" identifiers of the individual or of relatives, employers, or household members of the individual.

2. A data use agreement between the Corporation and the limited data set recipient will establish the permitted uses and disclosures of such information by the limited data set recipient; prohibit the limited data set recipient's use or disclosure of the information in a manner that would violate the privacy rules if done by the Corporation; establish who is permitted to use or receive the limited data set; and provide that the limited data set recipient will: (i) not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (ii) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (iii) report to the Corporation any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (iv) ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (v) not identify the information or contact the individuals.

F. Use of de-identified information or a limited data set. The Corporation will only use or allow the use of de-identified information or a limited data set in a limited manner that is in strict compliance with the Regulations and the Corporation will ensure, as applicable, that there are safeguards in place to protect again unintended re-identification and that a proper data use agreement is executed.

IV. DISCLOSURES TO FRIENDS AND RELATIVES

A. Basic rule. The Corporation may disclose to a person involved in the current health care of the patient (such as a relative, close personal friend, or any other person identified by the patient) PHI directly related to the person's involvement in the current health care of the patient or payment for the patient's health care.

B. Disclosures of PHI when the patient is present. When the patient is present and has the capacity to make his/her own decisions, the Corporation will disclose PHI to the third party only if the Corporation obtains the patient's agreement to disclose to the third party involved in his or her care.

C. Disclosures of PHI when the patient is not present. If the patient desires PHI to be disclosed to his/her family, a relative, a close friend or other person involved in the patient's health care or who has responsibility for payment for the patient's health care when the patient is not present or when the Corporation cannot practically give the patient an opportunity to agree or object to the disclosure to the third party, it is the Corporation's policy to require the patient's written authorization.

D. Limiting Disclosures to Third Parties. In the event of any disclosure to a third party, the PHI disclosed will be limited to the least amount of PHI directly necessary based on the third party's involvement with the patient's health care. For example, if a third party is accompanying the patient to be vaccinated under circumstances permitted under Section IV, the PHI disclosed should be limited to the information required to be provide along with the influenza and/or pneumonia vaccination without any further discussion or inclusion of PHI.

V. ORAL COMMUNICATIONS AND REASONABLE SAFEGUARDS

A. Applicability of privacy standards. The privacy rules apply to PHI in all forms – electronic, written, oral, and any other form.

B. Use of PHI in oral communications. Employees may orally coordinate Corporation services. Employees may discuss a patient's PHI over the telephone with the patient, a physician, or to a third party pursuant to the patient's written authorization.

C. Documentation of oral communications. The Corporation is not required to document any information, including oral information, which is used or disclosed for treatment, payment, or health care operations. However, oral disclosures of PHI for purposes other than treatment, payment, or health care operations will be documented in order to provide the patient with a complete accounting of disclosures.

D. The Corporation's duty to safeguard PHI. The Corporation will reasonably safeguard PHI, including oral information, from any intentional or unintentional uses or disclosures that are in violation of the rules or the Corporation's privacy policies. The Corporation will implement the following to protect patients' privacy:

1. Creating a private area, such as a small separate room, cubicle, or screened off or divided area, where consultation regarding vaccination and or other wellness services can occur.

2. Speaking quietly or asking that waiting patients stand a few feet back from the vaccine administration area when workforce members are consulting with patients.

3. Limiting the information that is disclosed if oral announcements must be made.

E. Procedures. The Corporation has created a system for recording oral disclosures of PHI that must be documented under the rules, which will provide a mechanism for documenting such oral disclosures in the patient's influenza vaccination and/or other wellness services record.

VI. DECEASED INDIVIDUALS

The Corporation will protect the PHI of deceased individuals in accordance with the Regulations and these Policies for as long as the Corporation maintains the PHI.

VII. PERSONAL REPRESENTATIVES

The Corporation will treat a person as the personal representative of a patient (and therefore, for purposes of these Policies, as the patient) if the person is, under applicable state or other law, authorized to act on behalf of the patient in making decisions related to health care. However, the personal representative will be treated as the patient only to the extent that PHI is relevant to the matters on which the personal representative is authorized to represent the patient.

5. PRIVACY PRACTICES

POLICY: It is the Corporation's policy to protect patients' PHI that is created, received, used, or maintained by the Practice in accordance with HIPAA and the Regulations.

PURPOSE: The purpose of this policy is to require the Corporation to name a Privacy Officer.

I. PRIVACY PRACTICES GENERALLY

A. Responsibility. The Corporation shall name a Privacy Officer who will be responsible for the development and implementation of these Policies and the policies and procedures that are designed to achieve ongoing compliance with the HIPAA Privacy Rule.

B. Relation to Security Officer. The Privacy Officer and Security Officer may be the same person.

6. SECURITY PRACTICES

POLICY: It is the Corporation's policy to protect patients' ePHI that is created, received, used, or maintained by the Practice in accordance with HIPAA and the Regulations.

PURPOSE: The purpose of this policy is to assure that appropriate procedures are in place to govern (1) record processing; (2) technical measures; and (3) physical access of ePHI.

II. SECURITY PRACTICES GENERALLY

C. Responsibility. The Corporation's Security Officer shall be responsible for the development and implementation of policies and procedures that are designed to achieve ongoing compliance with the HIPAA Security Rule.

D. Integrity. The Corporation's personnel shall protect ePHI against unauthorized access, alteration or destruction.

E. Risk Assessment. The Corporation shall perform an institutional security risk assessment to address HIPAA requirements as follows:

1. The Corporation shall perform system specific risk assessments of selected individual critical systems containing ePHI. These risk assessments shall be documented and shall provide a baseline for subsequent reviews.

2. On a continuing basis, the Corporation shall implement a process to identify ePHI systems or categories of systems and provide procedures by which the Corporation's Security Officer can assess compliance with security policies and procedures.

3. The Corporation shall review at least annually all systems and applications with ePHI and evaluate their vulnerabilities to threats as described in the Security Officer Responsibilities section below. Analysis must be done to determine what technical, physical and administrative safeguards are required and how best to implement those safeguards.

III. TECHNICAL AND ADMINISTRATIVE SAFEGUARDS

A. Technical Safeguards. The Corporation will institute appropriate technical safeguards described below. The adequacy of technical safeguards shall be reviewed regularly, no less than annually.

B. Administrative Safeguards. A range of administrative safeguards shall be instituted to protect ePHI. HIPAA Security Training is required for all personnel who create, access, store, transmit or receive ePHI or who access the Corporation network. Discipline, up to and including terminaton, will be imposed for noncompliance with these policies and procedures. The Security Officer monitors electronic information activity and audits compliance with HIPAA Security within the scope of his or her normal activities.

C. Passwords. All Corporation personnel must use "strong" passwords as identified by the Corporation's Information Technology ("IT") department for computer and application access.

D. Appropriate Use Policy. All Corporation personnel are prohibited from the sharing of accounts and passwords unless specifically authorized by the Security Officer and are prohibited from obtaining unauthorized access to Corporation IT systems or permitting others to do so.

E. Laptop and Desktop Configuration Standards. All Corporation laptop and desktop computers used to store, access or transmit ePHI must follow current secure configuration standards, including:

1. Whole disk encryption if containing any ePHI;

2. Automatic distribution of security and other patches via central computer management software;

3. Installation and update of anti-virus/anti-spyware software;

4. Automatic locking and password protection of desktops after a maximum of fifteen (15) minutes of inactivity;

5. Removal of applications that increase the vulnerability of computers;

6. Locking cables or equivalent physical protection (e.g. locked cabinets) for all devices when not in the user's physical custody; and

7. Other safeguards as they become technically feasible.

F. Smartphones and Other Mobile Data Devices. All Corporation personnel must implement current security standards for smartphones and other mobile data devices that create, store, access, transmit or receive ePHI, whether Corporation-issued or personal, including:

1. Use of a password with a minimum of four characters. The mobile data device must be set to delete all data or lock internally after 10 unsuccessful attempts to enter a password.

2. The data on mobile data devices must be encrypted. If data is backed up on another device that is not encrypted, the backup data must be encrypted.

3. No more than 200 messages or 14 days of messages on may be saved on a mobile data device at a given time.

4. Applications that create, store, access, send or receive ePHI must meet Corporation security standards.

5. All mobile data devices must use the most recent operating system available and must apply all available security updates unless otherwise instructed by the Security Officer.

6. All mobile data devices must be capable of remote deletion and locking.

7. Corporation personnel shall not circumvent the security of mobile data devices by removing limitations designed to protect the device.

G. WIRELESS NETWORKING

1. Corporation personnel must use the Corporation's VPN services when connecting to the Corporation network from a mobile data device.

2. Corporation personnel may only use secure WiFi networks known to be trustworthy. If a WPA-2 WiFi network cannot be used, then a VPN connection must be used to connect to the Corporation's network.

3. Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.

H. Removable Media Devices. Corporation personnel may never store ePHI on thumb drives or other removable media devices unless they meet Corporation encryption standards.

I. Personal Computers and Remote Access. Corporation personnel must not create, store, access, transmit or receive ePHI on personally owned computers. Personnel who require remote access to Corporation systems that hold ePHI must use a Corporation-provided, fully managed

and encrypted device, and must log-in via a virtual private network connection that is approved by the Security Officer.

J. File Transfer. All Corporation personnel may only forward ePHI data files or datasets outside the Corporation network, using an approved secure file transfer service.

K. Removal of ePHI. All Corporation personnel must securely destroy or delete ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives in accordance with Corporation policy.

L. Corporation Email Accounts. All Corporation personnel must not configure Corporation email accounts which may receive or transmit ePHI to auto-forward messages to non-Corporation email accounts.

IV. PHYSICAL SECURITY

A. Generally. Reasonable and appropriate physical security must be implemented to secure computing devices housing ePHI. These standards are applicable to all sites where Corporation ePHI may be created, accessed, transmitted, received, or stored.

B. Privacy Filters. Privacy filters must be installed on computer screens that display ePHI and can be viewed by the public or non-clinical staff.

C. Screensaver. A screensaver that hides the screen after 10 minutes of inactivity and requires a password to restore the display must be used.

D. Secure Office Space. Whenever possible, the office space must be secured through locking the room or area when a computer will be unattended for extended periods. A locking cable or equivalent physical protection (e.g. locked cabinets) shall be used for all devices when not in the user's physical custody.

E. Satellite Offices. Satellite offices, data centers, or on non-Corporation property that contain ePHI must be specified and adequate physical security implemented to ensure that only authorized individuals have access to ePHI systems.

V. SECURITY OFFICER RESPONSIBILITIES

A. Annual Assessment. The Security Officer shall perform a full security self-assessment of risks and vulnerabilities each year of its ePHI systems ("Annual Assessment").

B. Quarterly Assessment. The Security Officer shall evaluate the risks to the confidentiality, integrity and availability of the ePHI on a quarterly basis

and prior to any material change is made to a system or any new system is added.

C. Plan Development. The Security Officer shall determine what physical, administrative and technical safeguards may be necessary to adequately address the identified risks, based on the Annual Assessment, HIPAA Security policies and procedures, the Regulations, and other guidance. As appropriate, the Corporation must develop, document, implement and test a contingency plan that includes (1) a backup plan (2) an emergency mode operation plan; and (3) a disaster recovery plan.

VI. INVESTIGATION AND ENFORCEMENT PROCEDURES

A. Investigations. Reported violations will be investigated by the Security Officer. The Security Officer is also authorized to investigate security concerns identified through means other than a reported violation, including routine and targeted monitoring activities.

B. Disciplinary Measures. In addition to Corporation discipline, individuals found in violation of this Policy may be subject to criminal prosecution, civil liability, or both.

VII. EVALUATION

The Security Officer shall evaluate the technical and non-technical implementations of this Security Practices section. The purpose of this evaluation will be to determine the effectiveness of these policies as well as to ensure compliance with state and federal regulations such as HIPAA. The evaluation will be completed not less than once per year, as well as when any of the following events occur: (i) there is a change to any state or federal regulation that may affect these policies; (ii) there is a new state or federal regulation that may affect these policies; (iii) there has been a signification breach of security or other security incident; or (iv) any other time the Security Officer feels there is a need to evaluate these policies.

VIII. REPORTING VIOLATIONS AND POTENTIAL BREACHES

A. Reporting Generally. All Corporation personnel must immediately report violations and possible violations of this Policy and/or incidents that may involve the loss of, improper disclosure of, or improper access to ePHI (for example, the loss or theft of a computer, smartphone, or thumb drive storing ePHI; or an electronic intrusion into a computer storing ePHI). Reports should be made to the Corporation's Security Officer.

B. No Retaliation. Individuals who report violations in good faith must not be subjected to retaliation or harassment.

IX. ANNUAL COMPLIANCE

All Corporation personnel who create, store, access, transmit or receive ePHI must attest annually to full compliance with these policies. Failure to comply will result in disciplinary action.

7. AUTHORIZATION

POLICY: The Corporation will obtain a valid, signed authorization from a patient prior to using or disclosing the patient's PHI for purposes not otherwise permitted by a verbal agreement or the Regulations that allow uses or disclosures without the patient's permission.

PURPOSE: The purpose of this policy is to explain: (1) when a written patient authorization is required; and (2) the relevant procedures the Corporation will follow when using or disclosing PHI pursuant to a valid authorization.

I. WHEN AN AUTHORIZATION IS REQUIRED

A. An authorization is required before the Corporation uses or discloses PHI for purposes beyond treatment, payment and health care operations, such as sale of PHI and certain marketing activities.

B. An authorization is not required for uses and disclosures in connection with the following:

1. Treatment, payment, and health care operations;
2. Involvement in the patient's care and notification purposes;
3. Requirements of law;
4. Public health activities;
5. Preventing spread of communicable diseases;
6. Victims of abuse/neglect/domestic violence;
7. Health oversight activities;
8. Food and Drug Administration regulations;
9. Judicial and administrative proceedings;
10. Law enforcement purposes;
11. Decedents;
12. Research purposes where a waiver has been obtained;
13. Efforts to avert a serious threat to health or safety;

14. Specialized government functions;

15. Inmate care;

16. Workers' compensation;

17. Marketing communications that are made face-to-face or that involve promotional products of nominal value; or

18. Uses and disclosures to the patient or to the United States Department of Health and Human Services or its authorized representatives or any similar state agency or its authorized representatives or for enforcement of the Regulations.

II. CONTENT REQUIREMENTS

A. Plain language. All authorizations will be written in "plain language". The Corporation will make a reasonable effort to organize material to serve the needs of the reader; write short sentences in the active voice, using "you" and other pronouns; use common, everyday words in sentences; and divide material into short sections.

B. Core elements. Authorizations will contain all of the following core elements:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

3. The name or other specific identification of the person(s), or class of persons, to whom the Corporation will disclose the information.

4. A description of each purpose of the requested use or disclosure with enough information to allow patients to make informed decisions about whether to release the information. Broad or blanket authorizations requesting the use or disclosure of PHI for a wide range of unspecified purposes will not be used.

5. An expiration date or an expiration event that relates to the patient or the purpose of the use or disclosure. The authorization may expire on a specific date, a specific time period, or an event directly relevant to the patient or the

purpose of the use or disclosure, unless further limited by the Regulations. Authorizations will not have an indeterminate expiration date. Note that the expiration date must comply with both federal and state law.

6. Signature of the patient and date.

7. If the authorization is signed by a personal representative of the patient, a description of the representative's authority to act for the patient.

C. Required notifications. In addition to the core elements, authorizations will contain all of the following notifications:

1. A statement that the patient has the right to revoke the authorization in writing and either a discussion of the exceptions to the right to revoke together with a description of how the patient may revoke the authorization, or, to the extent that this information is included in the Notice, a reference to the Notice.

2. A statement that the Corporation will not condition treatment, payment, enrollment, or eligibility on the patient providing authorization for the requested uses or disclosures.

3. A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by the Regulations.

D. Authorizations for marketing. If the authorization is for a marketing purpose, and the marketing involves any direct or indirect remuneration to the Corporation from a third party, the authorization will state this fact.

E. Copy to the patient. The Corporation will give the patient a copy of the signed authorization.

F. Combining documents. An authorization for use or disclosure of PHI will not be combined with any other types of documents. However, multiple authorizations for the use or disclosure of PHI may be combined.

III. REVOCATION OF AUTHORIZATIONS

A patient may revoke an authorization at any time by means of a written revocation, except to the extent that the Corporation has taken action in reliance upon the authorization. When a patient revokes an authorization, the Corporation will stop making uses and disclosures pursuant to the authorization to the greatest extent practical.

IV. RECORD RETENTION REQUIREMENT

The Corporation will document and retain signed authorizations for six years after the date they were last in effect, or longer if required by the Regulations.

8. NATIONAL PRIORITY DISCLOSURES

POLICY: The Corporation may release PHI without a valid authorization or other permission from the patient if the use or disclosure falls within one or more of the national priority exceptions of the Regulations and the Corporation has complied with all of the conditions required by the exception.

PURPOSE: The purpose of this policy is to explain the situations where a national priority exception to the Regulations allows the Corporation to use or disclose PHI without a written patient authorization or oral permission, and to describe the relevant procedures the Corporation will follow when using or disclosing PHI in such situations.

I. RELEASE OF PHI FOR NATIONAL PRIORITY PURPOSES

A. General rule. The Corporation is allowed to use and disclose PHI for particular "national priority purposes" without obtaining any form of permission.

B. Specific situations where patient permission is not required. Listed below are separate categories of uses and disclosures for which the Corporation is not required to obtain affirmative permission from the patient prior to disclosure.

1. Required by law. The Corporation may use or disclose PHI as required by law, if the use or disclosure complies with and is limited to the relevant requirements of such law.

2. Public health activities. The Corporation may disclose PHI for the following public health activities: to a public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability (e.g., reporting communicable diseases), and the conduct of public health surveillance, investigations or interventions; and to a person subject to FDA jurisdiction regarding FDA regulated products and activities that are the responsibility of that person, for purposes related to the quality, safety or effectiveness of that product or activity.

3. Communicable diseases. The Corporation may disclose PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition

4. Health oversight activities. The Corporation may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, licensure or disciplinary actions; civil, administrative, or criminal proceedings; or other activities necessary for the oversight of the health care system, government benefit programs, or civil rights laws. The Corporation is permitted to respond to a health oversight agency's request for PHI as well as initiate these disclosures on its own.

5. Abuse or Neglect. The Corporation may disclose PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, the Corporation may disclose PHI if the Corporation believes that a patient has been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

6. Food and Drug Administration. The Corporation may disclose PHI to a person or Corporation as required by the Food and Drug Administration ("FDA") for purposes relating to the quality, safety or effectiveness of FDA regulated products or activities including, to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

7. Judicial and administrative proceedings. The Corporation may disclose PHI in the course of a judicial or administrative proceeding if the request for PHI is made pursuant to a court or administrative order or in response to a subpoena or discovery request (or other lawful process) from a party to the proceeding. If the request is made pursuant to a court or administrative order, the Corporation may disclose the information requested without additional process as long as proper notice has been given to the patient as required by the Regulations. In such cases, the Corporation may disclose only the information expressly authorized by the order and only if efforts have been made in accordance with the Regulations to notify the patient about the request or to obtain an order protecting the requested PHI. Without a court order or subpoena issued by a court, the Corporation will take additional steps to ensure the confidentiality of the information before it is permitted to disclose the minimum PHI necessary to fulfill the request.

8. Law enforcement purposes. The Corporation may disclose certain limited PHI for law enforcement purposes to a law enforcement

official under the following certain enumerated circumstances: to a law enforcement official as required by other law or court order, warrant, subpoena, or administrative request; to identify or locate a suspect, fugitive, material witness, or missing person; in response to a request about an individual who may be a victim of a crime; about an individual who has died as a result of criminal conduct; or where the Corporation believes that the information constitutes evidence of criminal conduct that occurred on the premises of the Corporation.

9. Coroners, Funeral Directors and Organ Donation. The Corporation may disclose PHI to a coroner or medical examiner for identification purposes, to determine cause of death or to perform other duties authorized by law. The Corporation may also disclose PHI to a funeral director, in order to permit the funeral director to carry out his/her duties. PHI may be used and disclosed for cadaver, organ, eye or tissue donation purposes.

10. Research. In certain circumstances, the Corporation may provide PHI in order to conduct medical research.

11. Specialized government functions. The Corporation may disclose the PHI of armed forces personnel if necessary for a military mission. The Corporation may also disclose PHI to federal officials for intelligence and national security activities, or to a law enforcement or correctional institution official who has custody of the individual and needs the information to provide health care to the individual or to protect the health and safety of others.

12. Inmates. The Corporation may use or disclose PHI if a patient is an inmate of a correctional facility and his/her physician created or received his/her PHI in the course of providing care to the patient.

13. Workers' compensation. The Corporation may disclose PHI as necessary to comply with laws relating to workers' compensation or similar programs.

14. Serious threat to health or safety. The Corporation may disclose PHI if it believes in good faith that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent the threat, or is necessary for law enforcement authorities to identify or apprehend an individual.

II. VERIFICATION OF IDENTITY AND AUTHORITY

A. Identity and author. With the exception of disclosures made pursuant to valid authorizations, prior to disclosing PHI the Corporation will verify

the identity of a person requesting PHI and the authority of such person to access PHI, if the identity and/or authority is not known.

B. Conditions on disclosures. The Corporation will obtain any documentation, statements or representations, whether oral or written, from the person requesting the PHI that are a condition of disclosure under the Regulations or other law.

C. Identity of public officials. The Corporation may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status. If the request is in writing, the request is on the appropriate government letterhead. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

D. Authority of public officials. The Corporation may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If a request is made pursuant to legal process, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.

III. PROCEDURES. The Corporation will only disclose PHI when it is legally required to do so as determined by the Privacy Officer and/or legal counsel and all disclosures of PHI pursuant to this National Priority Disclosures Policy shall only be made after approval of the Privacy Officer and/or legal counsel. The Corporation will maintain a log of these disclosures, which includes the name of the person/entity to whom PHI disclosed, the date of the disclosure, a description of the PHI disclosed and the purpose of the disclosure.

9. BUSINESS ASSOCIATES

POLICY: All agreements with business associates of the Corporation will be in writing and will contain certain mandatory provisions designed to protect the privacy and security of PHI. No Corporation employee shall disclose PHI to a business associate without a signed business associate agreement.

PURPOSE: The purpose of this policy is to protect, through the execution and enforcement of written agreements, the privacy and confidentiality of PHI that the Corporation discloses to individuals and entities that are business associates of the Corporation.

I. INTRODUCTION

A. Need for business associate agreements. From time to time, the Corporation contracts with an individual or Corporation to provide services to the Corporation or on behalf of the Corporation. If such a relationship involves sharing PHI that the Corporation maintains, then the Corporation will enter into a written contract, known as a "business associate agreement," with the individual or Corporation. The primary purpose of the agreement is to ensure that the business associate will use or disclose the PHI for lawful purposes only.

B. Limitations on the use of PHI. The business associate may only use the PHI that it receives in its capacity as the Corporation's business associate as permitted by the Regulations, other laws and its contract with the Corporation.

II. IDENTIFICATION OF A BUSINESS ASSOCIATE

A. Definition. A business associate is a person or entity that:

1. On behalf of the Corporation, performs or assists in the performance of functions or activities involving the use or disclosure of PHI. Examples of such functions may include but are not limited to claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management; or

2. Provides one of the following services to the Corporation where the provision of services involves the disclosure of PHI: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; financial.

B. Treatment exception. When the Corporation discloses PHI to other health care providers for the purpose of providing treatment to the patient, those health care providers are not considered business associates.

III. PROPOSED AGREEMENTS WITH BUSINESS ASSOCIATES

A. Proposed business associate agreements. Corporation employees must forward to the Privacy Officer all proposed agreements between the Corporation and an entity or individual pursuant to which the Corporation may provide access to PHI.

B. Review of proposed agreements. To determine whether a business associate agreement is required, the Privacy Officer and legal counsel will review each proposed agreement between the Corporation and an outside contractor if the contractor will use and disclose PHI pursuant to the agreement.

IV. REQUIRED ELEMENTS OF A BUSINESS ASSOCIATE AGREEMENT

A. A business associate contract will be in writing and will include provisions that:

1. Establish the permitted and required uses and disclosures of PHI by the business associate.

2. Prohibit other uses and disclosures by the business associate, except that the contract may permit the business associate to use and disclose PHI for the proper management and administration of its business and to provide data aggregation services for the Corporation.

3. Require appropriate safeguards to be implemented by the business associate to prevent inappropriate use or disclosure.

4. Require the business associate to report to the Corporation any inappropriate use or disclosure of PHI of which it becomes aware.

5. Require the business associate to mitigate, to the extent practicable, any harmful effect that becomes known to the business associate of a use or disclosure of PHI in violation of the business associate agreement.

6. Ensure that agents and subcontractors of the business associate who receive PHI from the Corporation also agree to the same restrictions and requirements with regard to use and disclosure of PHI.

7. Require the business associate to comply with HIPAA's requirement to allow individuals to review and copy their PHI.

8. Require the business associate to make available PHI in a designated record set for amendment and incorporate any amendments to PHI at the request of the Corporation.

9. Require the business associate to make available information that is required to provide an accounting of disclosures.

10. Require the business associate to make its internal practices, books, and records concerning PHI available to the United States Department of Health and Human Services.

11. Require the business associate to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Corporation.

12. Require the business associate to comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including but not limited to 45 CFR 164.316.

13. Require the business associate to report to the Corporation in writing any security incident of which the business associate becomes aware within two business days of becoming aware of such incident.

14. Provide for the return or destruction (or if not feasible, the continued protection) of all PHI by the business associate upon termination of the contract.

15. Authorize the Corporation to terminate the contract if the business associate violates a material term of the contract.

B. Optional provisions in the business associate contract. In addition to the required elements listed above, the business associate contract may also contain additional elements. The business associate contract may permit the business associate to use the PHI it receives from the Corporation for the proper management and administration of the business associate, or to carry out the legal responsibilities of the business associate, or if the disclosure is required by law; or the business associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law for the purpose for which it was disclosed to that person, and the person notifies the business associate of any instances of which the person is aware in which the confidentiality

of the PHI has been breached. The business associate contract may also permit the business associate to provide data aggregation services to the Corporation. The Privacy Officer and/or legal counsel will review the scope of the agreement to identify the permitted uses and disclosures as well as the data content that is minimally necessary to accomplish the function or activity performed by the business associate.

V. VIOLATIONS COMMITTED BY A BUSINESS ASSOCIATE

A. Employee's duty to notify. If an employee knows or has reason to believe that a business associate of the Corporation is inappropriately using or disclosing PHI, whether the PHI was received by the Corporation or not, the employee is required to notify the Privacy Officer immediately regarding the suspected violation.

B. Review of alleged violations. Upon receiving notice of an alleged or actual violation of a business associate agreement from any source, including notice obtained through patient complaints and employee reports, the Privacy Officer will initiate a review of the conduct or activities at issue. If the possible violation includes ePHI, the Privacy Officer shall involve the Security Officer.

C. Investigation and resolution of violations. If the Privacy Officer determines that the complaint, report or other form of notice contains substantial and credible evidence of violations by a business associate, the Privacy Officer will commence a formal investigation into the conduct or activities of the business associate. If the investigation reveals that a business associate has violated its agreement with the Corporation, the Privacy Officer shall notify legal counsel immediately. If the Privacy Officer and/or legal counsel determine that the business associate has committed a material breach or violation of its obligations under the business associate agreement, the Privacy Officer, with the assistance of legal counsel, will take reasonable steps to remedy the breach or terminate the contract of a business associate when feasible. If termination of the contract is not feasible, the Corporation will report the violation to the United States Department of Health and Human Services and any required state agencies.

10. MARKETING

POLICY: All Corporation marketing communications will comply with the Regulations' specific requirements.

PURPOSE: The purpose of this policy is to assist employees of the Corporation in complying fully with all of the complex Regulations governing marketing practices that involve PHI, while allowing employees the flexibility to best serve both the Corporation and its patients.

I. DEFINITION OF MARKETING

A. Marketing defined. Marketing is a communication about a product or service that encourages recipients of the communication to buy or use the product or service. Marketing specifically includes an arrangement between the Corporation and a third party whereby the Corporation discloses PHI, in exchange for direct or indirect remuneration, for the third party or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

B. Exceptions to the definition of marketing. Marketing does not include communications made by the Corporation for the patient's treatment; for case management or care coordination for the patient, or to recommend alternative treatments, therapies, health care providers, or settings of care; or to describe a health-related product or service (or payment for such product or service) that is provided by the Corporation, or included in a plan of benefits of a covered entity, including communications about the entities participating in a health care provider or health plan network, replacement of, or enhancements to, a health plan, and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

C. Other exceptions to the definition of marketing when payment is involved. Even if payment is involved, a communication will not be considered marketing if: the communication only describes a drug or biologic that has been previously prescribed or administered, provided the amount of the payment is reasonable; the Corporation makes the communication pursuant to an authorization from the recipient of the communication; or a business associate makes the communication pursuant to its business associate agreement.

D. Examples of exceptions. Examples of communications that should not be considered marketing include, but are not limited to, communications regarding the following: information regarding

insurance coverage and formularies; counseling; certain disease management activities; notifying patients about the Corporation's network participation; and general health information, such as communications that explain how to lower cholesterol or enroll in wellness programs.

II. USE AND DISCLOSURE OF PHI FOR MARKETING PURPOSES

A. General rule. A Corporation employee may use or disclose patient's PHI for marketing purposes only if the Corporation has obtained a valid, written authorization from the patient.

B. Exceptions to the general rule. A Corporation employee may use and disclose PHI without an authorization to make a marketing communication to a patient, if the communication occurs in a face-to-face encounter with the patient; or concerns promotional gifts of nominal value provided by the Corporation.

C. Format requirements. The authorization will conform in all respects with the requirements set forth in the Authorizations Policy set forth in these Policies. In addition, if the marketing involves direct or indirect remuneration to the Corporation from a third party, the authorization will state that such remuneration is involved.

D. Business associates and other third parties. The Corporation may engage a business associate to conduct marketing activities on its behalf. However, the Corporation will not sell or disclose PHI to a third party to help the third party market its own products or services without a signed authorization from the patient. That is, marketing occurs where an entity other than the Corporation (including a business associate of the Corporation) is promoting its own products using PHI it has received from, and for which it has paid, the Corporation.

E. Marketing communications. The following types of marketing communications may be utilized by the Corporation: in person, written, telephone, Internet, fax, and email. All formal marketing initiatives must be reviewed by the Privacy Officer.

11. REQUESTING ADDITIONAL PRIVACY

POLICY: It is the Corporation's policy to evaluate all patient requests for additional restrictions on the use and disclosure of their PHI on a case-by-case basis in compliance with the procedures set forth below. The Corporation will accommodate a patient's reasonable request to receive communications from the Corporation by alternative means or at alternative locations, if the patient specifies the alternative means or location.

PURPOSE: The purpose of this policy is to explain: (1) when a patient has a right to request that the Corporation restrict the use or disclosure of his/her PHI; (2) when a patient has a right to request that the Corporation send communications of PHI by alternative means or at alternative locations; and (3) the procedures that the Corporation will follow to handle these requests.

I. RIGHT TO REQUEST RESTRICTION OF USES AND DISCLOSURES

A. Patient's right to request restrictions. A patient may request additional restrictions on the Corporation's use and disclosure of his/her PHI when the PHI is used or disclosed to carry out treatment, payment, or health care operations; to persons assisting in the patient's care; or to friends, caregivers, or family members for notification purposes.

B. Written Requirement. The Corporation requires the patient to request additional restrictions of uses and disclosures in writing.

C. Agreeing to a restriction. The Corporation is not required to agree to a request for a restriction in all instances.

1. If the Corporation agrees to a restriction it will document the agreement, and will not use or disclose PHI in violation of the restriction except in the following circumstances: emergency treatment situations; disclosures permitted without a patient's permission; and disclosures made to the federal government during an investigation of the Corporation's compliance with the Regulations.

2. If the restricted PHI is disclosed in an emergency treatment situation, the Corporation will ask the health care provider to whom it is disclosed not to use or disclose the PHI for other purposes.

D. Terminating a restriction. The Corporation may terminate its agreement to a restriction if the patient agrees to or requests the termination in

writing; the patient orally agrees to the termination and the Corporation documents the oral agreement by a notation in the patient's record or similar documentation; or the Corporation informs the patient that it is terminating its agreement to the restriction. In this situation, the termination is effective only for the PHI created or received after the Corporation has informed the patient of the termination.

E. Generally acceptable restrictions. All requests for restrictions will be reviewed and approved by the Privacy Officer in accordance with these Policies and the Regulations.

F. Procedures. The Corporation will document any restrictions that are agreed to. The Corporation will notify the patient in writing of its determinations within 60 days of the Corporation's receipt of the request, and it will disseminate the restrictions to the appropriate persons within the Corporation for implementation as promptly as practicable.

II. RIGHT TO REQUEST ALTERNATIVE COMMUNICATIONS

A. Patient's right to request alternative communications. The Corporation will accommodate reasonable requests by patients to receive communications of PHI from the Corporation by alternative means or at alternative locations.

B. Writing requirement. The Corporation requires the patient to make a request for alternative communication in writing.

C. Refusing requests. The Corporation may refuse to accommodate a request if the patient has not provided information as to how payment, if applicable, will be handled, or has not specified an alternative address or other method of contact.

D. Reasons for requests. The Corporation will not require the patient to give a reason for the request as a condition of accommodating the request.

E. Procedure. The Privacy Officer will review all requests, and will communicate with the patient within 60 days after the Corporation's receipt of the request whether the request will be accepted or refused. The Privacy Officer will inform all personnel who, as part of their job functions, need to communicate with the patient by alternative means or at alternative locations as soon as practicable.

III. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

The Corporation will document any restriction that it accepts, and will retain the documentation until six years after the date the restriction was last in effect, or longer if required by the Regulations.

12. RIGHT TO ACCESS RECORDS

POLICY: The Corporation shall process, in accordance with the procedures outlined below, a request to access, inspect, and/or obtain a copy of certain PHI maintained by the Corporation, if the request is made by a patient or his/her personal representative.

PURPOSE: The purpose of this policy is to establish a process for patients to access, inspect and obtain a copy of certain PHI maintained by the Corporation.

I. RIGHT OF ACCESS TO PHI

A. Basic right to access. In general, a patient has a right to request access to, inspect, and obtain a copy of his/her PHI held by the Corporation, for as long as the PHI is maintained by the Corporation. Exceptions to the right of access are set forth below.

B. Written Requests. The Corporation requires the patient to make requests for access in writing. The Corporation will inform patients of this requirement and will apply the policy uniformly.

C. Denials without an opportunity for review. The Corporation may deny the patient's request for access without providing the patient an opportunity for review of the decision in any of the following circumstances:

1. The PHI was compiled by the Corporation in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

2. The PHI was obtained by the Corporation in the course of research that includes treatment of the research participants, while such research is in progress, and the patient previously agreed to this temporary suspension.

3. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

D. Denials with an opportunity for review. The Corporation may deny the patient access, so long as the patient is given a right to have the denial reviewed, in any of the following circumstances:

1. If the request for access is made by the patient's personal representative and a licensed health care professional has

determined, in the exercise of professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the patient or another person.

2. If the PHI consists of mental health medical records for which a treating physician, psychologist, or mental health practitioner has determined in his or her professional opinion, and the Corporation has been made aware of, that the release of such PHI would not be in the best interest of the patient.

E. Right to review of denial. If the Corporation denies the patient access to his or her PHI as described in Section 10(I)(D) above, the patient has the right to have the denial reviewed by a licensed health care professional who is designated by the Corporation to act as a reviewing official and who did not participate in the original decision to deny access. The Corporation will provide or deny access in accordance with the determination of that official.

F. Verification. Prior to disclosing PHI to a person unknown to the Corporation, the Corporation will verify the identity of the person requesting the PHI and the authority of the person to have access to the PHI requested. In addition, the Corporation will obtain any documentation, statements, or representations, whether oral or written, from the requestor when such information is a condition of the disclosure. Verification methods include, but are not limited to, obtaining a copy of a driver's license, passport or birth certificate. If the person requesting the PHI is not the patient, the Corporation will require a signed Authorization form from the patient prior to disclosure of the PHI.

II. RESPONDING TO A REQUEST FOR ACCESS

A. Acting on the request. The Corporation will act on a request for access within 10 days of the date the Corporation received the request.

1. If the Corporation grants the patient's request for access, it will inform the patient that the request has been granted and provide access to the PHI in accordance with subsection (B) below.

2. If the Corporation denies the patient's request for access, it will provide the patient with a written denial in accordance with subsection (C) below.

3. If the PHI does not exist or cannot be found, the Corporation will provide the patient with a written denial.

4. If the Corporation does not maintain the PHI, it will provide the patient with a written statement of the name and address of the provider who maintains such PHI, if known.

B. Provision of access. If the Corporation grants a request for access, it will comply with the following requirements.

1. The Corporation will notify the patient and provide the access as requested, including inspection or obtaining a copy, or both, of the PHI.

2. The Corporation will provide the patient with access to the PHI in the form or format requested by the patient, if it is readily producible in this form or format; or if not, in a readable hard copy form or other form that is agreed upon by the Corporation and the patient.

3. If acceptable to the patient and the Corporation, the Corporation may provide the patient with a summary or explanation of the PHI instead of providing access to the actual PHI.

4. The Corporation will provide access in a timely manner, but not later than ten (10) days after receiving the request, including arranging with the patient for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the patient's request. If unusual circumstances have delayed the handling of the request within ten (10) days after receiving the request, the Corporation will inform the patient in writing of the reasons for the delay and the earliest date, not later than twenty-one (21) days after receiving the request, when the PHI will be available for examination. The Corporation may discuss the scope, format, and other aspects of the request for access with the patient as necessary to timely provide access.

5. If the patient requests a copy of the PHI or agrees to a summary or explanation, the Corporation may charge a reasonable, cost-based fee, provided that the fee includes only the cost of copying, postage, and preparing an explanation or summary of the PHI (if a summary is requested by the patient). The fee will not include costs associated with searching for and retrieving the records.

C. Denial of access. If the Corporation denies access to PHI, it will implement the following procedures:

1. Give the patient access to any other PHI requested, to the extent possible, after excluding the PHI that the Corporation has grounds to deny access.

2. Provide a timely, written denial to the patient within the time frame referenced above. The denial will be in plain language and will include (i) the basis for the denial; (ii) if applicable, a statement of the patient's right to review of the decision, including a description of how the patient can exercise these review rights; and (iii) a description of how the patient may complain to the Corporation or the Secretary of Health and Human Services, including the name or title and telephone number of the contact person or designated office.

3. Inform the patient where to direct the request for access, if the Corporation does not maintain the PHI that is the subject of the patient's request for access, and the Corporation knows where the requested information is maintained.

4. If the patient has requested a review of a denial, the Corporation will designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access. The Corporation will promptly refer the review request to the reviewing official. The reviewing official will determine, within a reasonable period of time, whether or not to deny access. The Corporation will promptly provide written notice to the patient of the reviewing official's decision and carry out the decision.

III. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

The Corporation will document the records that are subject to access by patients and the titles of the persons or offices responsible for receiving and processing requests for access. The Corporation will retain this documentation from the date of its creation until six years after the date when it was last in effect.

13. REQUESTING AMENDMENTS

POLICY: It is the Corporation's policy to respond to a patient's request for an amendment to his/her PHI held by the Corporation (and/or by the Corporation's business associates, if any) in compliance with the Regulations.

PURPOSE: The purpose of this policy is to establish a process for responding to patient requests to amend PHI maintained by the Corporation.

I. RIGHT TO AMENDMENT OF PROTECTED HEALTH INFORMATION

A. Patient's right to amendment. A patient has the right to request that the Corporation amend PHI about the patient that is contained in the Corporation's records for as long as the PHI is maintained by the Corporation.

B. Accepting a patient's request for amendment. If the Corporation has no grounds to deny the patient's request for amendment *(see* Section 11(I)(C) below), the Corporation will do all of the following:

1. Make the appropriate amendment to the patient's PHI or record. The Corporation will, at a minimum, identify the records that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

2. Inform the patient on a timely basis that the amendment is accepted and obtain the patient's identification of and permission to have the Corporation notify the relevant persons with whom the amendment needs to be shared.

3. Make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the patient as having received PHI and needing the amendment; and persons, including business associates, that the Corporation knows have the unamended information and may have relied, or might rely in the future, on the information to the detriment of the patient.

C. Denying a patient's request for amendment. Under certain circumstances, the Corporation may deny the patient's request for amendment to his or her PHI held by the Corporation.

1. Permissible reasons for denial. The Corporation may deny a request for an amendment only for any of the following reasons:

a. The PHI was not created by the Corporation, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.

b. The PHI is not part of the patient's designated record set.

c. The PHI would not be available for inspection under the Corporation's policy regarding the patient's right to access to records.

d. The PHI is accurate and complete.

2. Denial procedures. If the Corporation denies the requested amendment, in whole or in part, the Corporation will take the following steps.

a. The Privacy Officer will provide the patient with a valid, written denial that explains the basis for the denial; how the individual may file a written statement disagreeing with the denial; the individual's options with respect to future disclosures of the disputed information; and how the individual may make a complaint to the United States Department of Health and Human Services.

b. The Corporation will permit the patient to submit to the Corporation a one (1) page written statement disagreeing with the denial and the basis for the disagreement. The Corporation may prepare a written rebuttal to the patient's statement of disagreement. If the Corporation prepares a rebuttal, it will provide a copy to the patient.

c. The Corporation will identify, as appropriate, the information in the patient's record that is the subject of the disputed amendment and append or otherwise link to this information the patient's request for an amendment, the Corporation's denial of the request, the patient's statement of disagreement, and the Corporation's rebuttal to the information.

d. The Corporation will adhere to the following guidelines if it makes future disclosures of the patient's disputed PHI. If the patient has submitted a statement of disagreement, the Corporation will include either the material appended to the record, or an accurate summary of it, with any subsequent disclosure of the PHI to which the disagreement relates. If the patient has not submitted a written statement of disagreement, the Corporation will

include the appended information with any subsequent disclosure only if the patient has requested that the Corporation do so.

D. Receiving a notice of amendment from other health care providers or health plans. Other health care providers or health plans may contact the Corporation to let it know that they have made amendments to the patient's PHI. When the Corporation is informed by another health care provider or health plan of an amendment to a patient's PHI, the Corporation will make necessary amendments to the PHI in its records.

E. Time period for acting on requests. The Corporation will act on the patient's request for an amendment within 60 days of receipt of the request. If the Corporation is unable to act on the amendment within 60 days, the Corporation may extend the time period once for 30 days, if within the original 60 day time limit the Corporation provides the patient with a written statement of the reasons for the delay and the date by which the Corporation will complete its action on the request.

II. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

The Corporation will document the titles of the persons or offices responsible for receiving and processing requests for amendments by patients; until so designated, the Privacy Officer shall be such office. The Corporation will also document requests for amendments and the resolution of those requests. The Corporation will retain this documentation from the date of its creation until six years after the date when it was last in effect, or longer if required by the Regulations.

14. ACCOUNTING OF DISCLOSURES

POLICY: It is the Corporation's policy to provide patients, upon request, a timely accounting of certain disclosures of their PHI as required by law and the Regulations.

PURPOSE: The purpose of this policy is to establish a process by which the Corporation will respond to patients' requests for an accounting of the Corporation's disclosures of their PHI.

I. RIGHT TO AN ACCOUNTING OF DISCLOSURES

A. Basic right to an accounting. The patient has a right to receive an accounting of disclosures of his/her PHI made by the Corporation and its business associates for the six (6) year period prior to the date of the request, or longer if required by the Regulations. Such requests should be submitted on the form provided by the Corporation to the Privacy Officer.

B. Exceptions to the basic accounting requirement. The Corporation is not required to provide an accounting of disclosures that were made by the Corporation:

1. For purposes of treatment of the patient;

2. For payment activities, including billing, claims management, eligibility determinations, coordination of benefits, determination of cost-sharing amounts, and adjudication of health benefit claims;

3. For health care operations, including management and administrative activities, patient service, quality assessment and improvement, training programs, auditing, compliance, business planning and development, and certain due diligence activities conducted in connection with the sale or transfer of assets;

4. To the patient requesting the accounting;

5. To individuals involved in the patient's care where the patient verbally agreed to the disclosure;

6. To authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and certain other national security activities;

7. To a correctional institution or law enforcement official, upon a request by, and during such time as, the correctional institution or law enforcement official had lawful custody of the patient;

8. Incident to a use or disclosure that is otherwise permitted by the privacy rules;

9. Pursuant to a valid patient authorization; or

10. As part of a limited data set that was disclosed pursuant to a data use agreement for purposes of research, public health or health care operations.

C. Electronic PHI accounting requirement. If the Corporation utilizes an electronic health record ("EHR"), the patient has a right to receive an accounting of disclosures of his/her PHI used or maintained in such EHR that are related to treatment, payment or health care operations for a period of three years prior to the date of the request. Note that the effective date of this requirement will depend upon when the Corporation obtains its EHR. If the Corporation had EHR as of January 1, 2009, the Corporation must comply with this requirement starting January 1, 2014. If the Corporation acquired EHR after January 1, 2009, the effective date of this requirement is the later of January 1, 2011, or the date the EHR is acquired.

D. Suspension of accounting. A health oversight agency or law enforcement official may request that the Corporation temporarily suspend the patient's right to receive an accounting of disclosures made to the health oversight agency or law enforcement official. Upon appropriate request, the Corporation will temporarily suspend a patient's right to receive an accounting of these disclosures for the time specified by such agency or official, if such agency or official provides the Corporation with a written statement that (i) an accounting to the patient would be reasonably likely to impede the agency's activities; and (ii) specifies the time period for which a suspension is required. But if that agency or official statement is made orally to the Corporation, the Corporation will document the statement, including the identity of the agency or official making the statement; temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement from the agency or official is submitted during that time.

E. Time period for action. The Corporation will act on a patient's request for an accounting no later than 30 days after receipt of such a request by providing the patient with the accounting requested; or if the Corporation is unable to provide the accounting within 30 days of receipt of the request, the Corporation may extend the time to provide the

accounting once, by no more than 30 days, if the Corporation, within 30 days of receipt of the request, provides the patient with a written statement of the reasons for the delay and the date by which the Corporation will provide the accounting.

F. Fees for providing an accounting. The Corporation will provide the first accounting to a patient in any 12-month period without charge. The Corporation may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the same 12-month period. If a fee will be charged, the Corporation will inform the patient in advance of the fee and provide the patient an opportunity to withdraw or modify the request for a subsequent accounting to avoid or reduce the fee.

II. REQUIRED CONTENTS OF AN ACCOUNTING OF DISCLOSURES

A. Core elements. An accounting of disclosures will be in writing and will contain the following elements for each disclosure:

1. The date of the disclosure;

2. The name of the entity or person who received the PHI;

3. The address of the entity or person who received the PHI, if unknown;

4. A brief description of the PHI disclosed; and

5. Either (a) a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure, or (b) a copy of a written request for a disclosure made pursuant to the Corporation's policy for disclosures to government entities.

B. Multiple disclosures. For certain disclosures that occur on a regular basis, other than disclosures listed in section 12(I)(B) above, the Corporation may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure.

1. When a summary accounting is permissible. A summary accounting for multiple disclosures is permissible if during the period covered by the accounting, the Corporation has made multiple disclosures of PHI for a single purpose to the United States Department of Health and Human Services so it may investigate or determine the Corporation's compliance with the roles; or to the same person or entity for a single national priority purpose (as set forth in the Corporation's policy regarding national priority disclosures).

2. Required information for a summary accounting. Rather than include all of the core elements listed in section 12(II)(A) above for every disclosure in a series of disclosures, the Corporation may limit the accounting to the core elements (set forth in Section 12(II)(A) above) for the first disclosure during the accounting period; the frequency or number of the disclosures made during the accounting period; and the date of the most recent disclosure in the series during the accounting period.

III. RECORD RETENTION REQUIREMENTS

A. Required documentation. The Corporation will create and maintain the following documentation: the core elements of each disclosure as set forth in Section 12(II)(A) above; the written accounting that is provided to the patient; and the titles of the persons or offices within the Corporation responsible for receiving and processing a patient's request for an accounting.

B. Retention period. The Corporation will retain the required documentation for a period of six (6) years from the date of its creation or the date when it was last in effect, whichever is later, or longer if required by the Regulations.

15. NOTIFICATION OF BREACH

POLICY: It is the Corporation's policy to provide notification to the proper parties in the event of a breach of security of the PHI of one or more individuals.

PURPOSE: The purpose of this policy is to establish a process by which the Corporation will respond to a security breach and notify the proper parties in the event of a breach in accordance with applicable law.

IV. SECURITY BREACH NOTIFICATION

A. Breach of "unsecured" PHI. The Corporation will only provide notification of a security breach if the breach involves "unsecured" PHI. For PHI to be secured, it must be rendered unusable, unreadable or indecipherable to unauthorized individuals by "encryption" in accordance with standards specified under the HIPAA Security Rule, or the media on which the PHI is stored must be destroyed in one of several ways. The procedures discussed below do not apply to secured PHI. PHI that does not meet the secured PHI standards is "unsecured".

B. Notification to individuals. If the Corporation has reasonable belief that an individual's PHI has been involved in a breach, the Corporation must notify each individual personally. The Privacy Officer will make this determination. The Corporation will provide notice by first class mail to the individual's last known address unless the individual agreed to receive such notice electronically. Notification to an affected individual will contain the following information:

1. A brief description of what happened, including the date of breach and the Corporation's date of discovery of the breach, if known.

2. A description of the types of "unsecured" information that were involved in the breach. Actual protected information should not be included. For example, the notice of breach should state that the individual's Social Security number was involved in the breach, but should not list the individual's actual Social Security number.

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what the Corporation is doing to investigate, mitigate harm to individuals, and protect against further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, including either a toll-free telephone number, email address, website or postal address.

Notifications to individuals must be sent no later than 60 calendar days from the date the Corporation discovers the incident that is ultimately determined to constitute a breach. Urgent notice and substitute notice may be provided in urgent situations or where current contact information is not available.

C. Notification to the media. If a breach affects 500 or more individuals within a state or jurisdiction, the Corporation must provide notice to a prominent media outlet within that state or jurisdiction. "Jurisdiction" means a geographic area smaller than a state, such as a county, city or town. The notification to media is in addition to, and not a substitute for, the individual notice or substitute notice, and should include the same content as the substitute notice.

1. Notification to the Secretary of Health and Human Services. If the Corporation discovers a breach involving 500 or more individuals, the Corporation must immediately report the breach to the Secretary of Health and Human Services (the "Secretary") in accordance with instruction posted on the Department of Health and Human Services' website.

D. If the Corporation discovers a breach involving less than 500 individuals, the Corporation must maintain a log of tracking all breaches of unsecured PHI (even if the breach only involves one person) and report the contents of the log to the Secretary annually no more than 60 days after the end of the calendar year.

16. TRAINING

POLICY: All members of the Corporation's workforce will receive training regarding the Corporation's privacy policies and procedures as necessary and appropriate for each member of the workforce to carry out his or her functions within the Corporation. All members of the Corporation's workforce will also receive training regarding the Corporation's change management program for the Corporation's privacy policies and procedures.

PURPOSE: The purpose of this policy is to ensure that the workforce receives effective and timely education regarding the Corporation's privacy policies and procedures, as well as the change management program related to the same, and that an education curriculum is created and maintained to meet the needs of Corporation employees.

I. TRAINING

A. Initial training. Members of the Corporation's workforce will complete an updated privacy and security training program by December 31, 2013. Completion of this updated privacy and security training is mandatory and will be considered when workforce members are evaluated during performance reviews. Failure to complete privacy and security training will result in disciplinary action.

B. New workforce members. As part of their initial orientation, new workforce members will receive privacy and security training.

C. Additional training. When material changes are made to a policy or procedure, all members of the workforce whose functions are affected by the change will receive training on the new policies and procedures within a reasonable time after the material change has been made.

D. Content of training. In training, workforce members will review the Corporation's privacy and security policies and procedures and will discuss any changes in these policies and procedures. The training program will focus on federal laws and regulations governing the privacy, confidentiality, and security of PHI, as well as any more stringent state laws. Training program subjects and materials will be updated on a regular basis to comply with all applicable law.

E. Documentation requirements. The Corporation will document that the required training has been provided.

F. Training Mechanics. The Privacy Officer, Security Officer (if different), and/or legal counsel will be primarily responsible for conducting training

programs. This HIPAA compliance policy and procedure manual will be used in the training programs. Upon completion of training, each employee will sign a certificate acknowledging such completion, which will be retained by the Corporation.

17. PATIENT COMPLAINTS

POLICY: Because customer service and privacy are of utmost importance to the Corporation, it is our policy to promptly receive, respond, and resolve complaints regarding allegations of improper use or disclosure of PHI by the Corporation or our business associates.

PURPOSE: The purpose of this policy is to establish a process for the receipt and resolution of privacy-related complaints.

I. GENERAL RULE

A. Subject of complaints. An individual may lodge a formal complaint about the Corporation's information practices, including but not limited to complaints regarding the privacy and security of PHI; use and disclosure of PHI; patients' access to, or amendment of, their PHI; practices or actions of the Corporation's business associates; the Corporation's marketing practices; or any other complaint relating to the Corporation's privacy policies and procedures.

B. Documentation of complaints. The Corporation will maintain complete documentation of the complaint and the Corporation's review and disposition of the matter, including a record of any changes to policies or procedures or the imposition of sanctions against members of its workforce, if any. The Corporation will retain all documents relating to the complaint and the investigation for a period of at least six years after the date of their creation.

II. PROCEDURES

A. Contact Person. The Corporation's employees will explain to the individual that the Corporation has established a contact person, the Privacy Officer, to receive and respond to privacy-related complaints.

B. Complaints. Upon receipt of a complaint in person, via telephone or in writing, the Corporation employee will give/send the individual a copy of the Corporation's notice of privacy practices, and point out the section that explains the process for submitting privacy related complaints to the Corporation.

C. Review of Complaints. The Privacy Officer will review and respond to complaints within 60 days after the Corporation's receipt of the complaint. The Corporation will communicate the results of its review to the individual in writing, explaining the Corporation's determination and resolution of the complaint.

18. INTERNAL ENFORCEMENT

POLICY: This sanctions policy addresses violations of federal and state privacy laws and these Polices ("Violations" or a "Violation") by members of the Corporation's workforce. The Human Resources Director, in consultation with the Privacy Officer, will administer any appropriate sanctions related to Violations, consistent with the procedures established below.

Appropriate sanctions may be based on factors such as the severity, frequency, degree of deviation from expectations, and length of time involved in any violations. Whether to impose sanctions, and the appropriate sanctions to impose, are always within the discretion of the Corporation. Violations may result in disciplinary action, including but not limited to informal counseling, verbal warning, written warning, probation, suspension, demotion, dismissal and/or restitution. However, progressive discipline is not a right. The Corporation reserves the right to terminate employment at any time, for any reason, with or without undertaking any of the progressive disciplinary actions outlined in this policy. In light of the variety of possible situations that may arise, the Corporation may need to make decisions related to employment in a manner other than as provided in this section.

PURPOSE: The purpose of this policy is to establish written guidelines for undertaking disciplinary action against employees who violate federal or state privacy laws or these Policies.

I. GENERAL RULES

A. Members of the Corporation's workforce are encouraged to report possible Violations to the Privacy Officer.

B. Whenever possible Violations arise, the Privacy Officer will conduct an investigation and determine whether a violation has occurred. If the possible Violations include ePHI, then the Privacy Officer shall involve the Security Officer in all aspects of compliance with this policy.

C. If the Privacy Officer determines that an employee has committed a Violation, that employee shall be subject to appropriate sanctions as determined by the employee's immediate supervisor, the Privacy Officer, the Human Resources Director, or legal counsel. Even if no actual Violation has occurred, disciplinary measures may be imposed if otherwise warranted by the circumstances.

D. The sanctions imposed may include, but are not limited to, informal counseling, verbal warning, written warning, suspension or termination. An employee may also be placed on probation or demoted. Restitution

will be required if appropriate in the circumstances. In all cases, the sanction imposed will be in the discretion of the Privacy Officer. In most cases the sanction will depend on the seriousness of the offense, among other factors. *See* Section II below.

E. A manager or supervisor may also be sanctioned to the extent that inadequate supervision or a lack of due diligence contributed to the violation, or if the manager or supervisor's conduct was culpable or sanctionable in other ways. Managers and supervisors may be sanctioned for failing to detect noncompliance with applicable policies and legal requirements, where reasonable diligence would have led to the discovery of any problems or violations.

F. A record of the event and any discipline imposed shall be maintained in the employee's personnel file with a copy to be filed in a master file maintained by the Privacy Officer.

II. EXAMPLES OF POSSIBLE SANCTIONS

The following summarizes the types of sanctions that may be imposed by the Corporation if a Violation has occurred. Progressive discipline is not a right, and the Corporation reserves the right to impose discipline or to terminate employment at any time, for any reason, with or without undertaking any of the lesser sanctions outlined in this policy. The type of sanctions imposed will generally reflect the seriousness of the problem or violation. Factors may include the severity, frequency, degree of deviation from expectations, and length of time involved in any Violations. Some offenses, such as intentional violations, are so serious that they will justify termination or suspension on the first offense. For offenses that may not justify serious discipline on the first offense, lesser sanctions may be applied in the discretion of the Corporation.

A. Informal Counseling. The Privacy Officer may engage in informal counseling with respect to privacy issues that do not warrant more severe sanctions. Documentation of informal counseling may be maintained in personnel and departmental files.

B. Verbal Warning. The Privacy Officer may issue a verbal warning to an employee. Documentation of the verbal warning will be maintained in personnel and departmental files.

C. Written Warning. The Privacy Officer may issue a written warning to an employee. Such a warning may be appropriate, for example, when the behavior of the employee is a repeated violation and verbal counseling has been administered, or the violation is more serious in nature and/or subjects the Corporation to potential legal liability. Written warnings will be documented in personnel and departmental files.

D. Probation. In appropriate circumstances, an employee may be placed on probation for a specified period of time. When probation is imposed, the employee will generally be provided with a written description of the behavior that resulted in the probation and the required behavioral or performance objectives that will be met in order to remove the employee from probation. Copies of documents relating to probations will be kept in personnel and departmental files.

E. Suspension. Suspension, or temporary release from duty, is a more severe action that may be imposed in the discretion of the Corporation. Suspension may also be used during investigations in order to more easily conduct such investigations. Suspensions may be issued when, in the discretion of the Corporation, it is determined that a second warning would not suffice or that an initial incident is too severe for a warning yet not sufficiently severe for termination. Suspensions may vary in length, according to the severity of the Violation. Suspensions may be paid or unpaid, in the discretion of the Corporation and consistent with applicable laws. Suspensions will be documented in personnel and departmental files.

F. Demotion. In appropriate circumstances, an employee may be demoted (transferred to a lower-level position) as a sanction for Violations. Demotions will be documented in personnel and departmental files.

G. Termination of Employment. Termination of employment is generally the most serious disciplinary sanction for Violations. Employment with the Corporation is at-will, and may be terminated at any time, for any reason, in the discretion of the Corporation. Termination as a disciplinary sanction may, for example, be imposed after other disciplinary measures have failed or when a first time incident occurs that is extremely serious. Copies of relevant documentation pertaining to terminations will be maintained in personnel and departmental files.

H. Restitution. Where an employee's Violation has caused harm or damage to the Corporation or its patients, sanctions may include restitution to the Corporation or its patients.

III. ACTIONS THAT MAY RESULT IN SANCTIONS

Without limiting the Corporation's right to discharge an employee at any time, with or without cause, the following acts of misconduct are provided as nonexclusive examples of unacceptable activity that may result in sanctions up to and including termination: misuse or theft of PHI, with or without the intent to unlawfully sell the information to an outside party; failure to properly maintain an up-to-date accounting of instances in which the Corporation has released a patient's PHI to a third party; discussion of the patient's conditions in the presence of unrelated third parties; or use of unapproved marketing materials.

19. REVIEW OF POLICIES

POLICY: The Corporation will review the Policies on a regular basis, not less frequently than annually.

Revisions and/or updates to the Policies will be made and approved by the Corporation as needed. The Corporation's legal counsel may lead or take part in such reviews.

PURPOSE: The purpose of this policy is to establish written guidelines for regular reviews of the Policies to ensure compliance with applicable law at all times.

III. GENERAL RULES

A. The Corporation's Board of Directors shall meet with the Privacy Officer and Security Officer at least annually to review the Policies.

B. The Corporation's legal counsel may be a part of such meetings and propose recommended compliance updates.

C. The Board of Directors shall discuss and ratify revisions and/or updates to the Policies as necessary.

EXHIBIT A

VACCINATION SERVICES OF AMERICA, INC. d/b/a TOTALWELLNESS
NOTICE OF PRIVACY PRACTICES
Effective June 1, 2011

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" or "PHI" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

We are required to maintain the privacy of your PHI and to provide you with notice of our legal duties and privacy practices with respect to your PHI. We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice at any time. The new notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with any revised Notice of Privacy Practices. You may request a revised version by accessing our website or by contacting our Privacy Officer at the telephone number or address listed at the end of this notice.

1. **Uses and Disclosures.** The law allows us to use and disclose your health information for treatment, payment and health care operations. The following are examples of such uses and disclosures:

    a. Treatment. We may use or disclose your PHI to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with another provider. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you.

    b. Payment. We may use or disclose, as needed, your PHI to obtain payment for your health care services provided by us or another provider. For instance, we may forward information regarding your health status to your insurance company to arrange payment for the services provided to you or we may use your information to prepare a bill to send to you or to the person or entity responsible for your payment.

    c. Health Care Operations. We may use or disclose, as needed, your PHI to operate our business. These activities include, but are not limited to, quality assessment and improvement activities.

    We will share your health information with third party "business associates" that perform various activities on our behalf. Whenever an arrangement between our office and a business associate involves the use or disclosure of your PHI, we will have a written contract that contains terms that will protect the privacy of your PHI.

We may use or disclose your PHI to provide you with information about health-related benefits and services that may be of interest to you. You may contact our Privacy Officer in writing to request that these materials not be sent to you.

2. **Uses and Disclosures Allowed or Required by Law**. We may use or disclose your health information in the following situations as allowed or required by law:

   a. Required By Law. We may use or disclose your PHI to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, if required by law, of any such uses or disclosures.

   b. Public Health. We may disclose your PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury or disability.

   c. Communicable Diseases. We may disclose your PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

   d. Health Oversight. We may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections.

   e. Abuse or Neglect. We may disclose your PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

   f. Food and Drug Administration. We may disclose your PHI to a person or company as required by the Food and Drug Administration ("FDA") for purposes relating to the quality, safety or effectiveness of FDA regulated products or activities including, to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

   g. Legal Proceedings. We may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.

   h. Law Enforcement. We may disclose PHI, so long as applicable legal requirements are met, for law enforcement purposes.

   i. Coroners, Funeral Directors and Organ Donation. We may disclose PHI to a coroner or medical examiner for identification purposes, to determine cause of death or to perform other duties authorized by law. We may also disclose PHI to a funeral director, in order to permit the funeral director to carry out his/her

duties. PHI may be used and disclosed for cadaver, organ, eye or tissue donation purposes.

j. Research. In certain circumstances, we may provide PHI in order to conduct medical research.

k. Criminal Activity. Consistent with applicable federal and state laws, we may disclose your PHI, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

l. For Specific Government Functions. We may disclose PHI of military personnel and veterans in certain situations. We may also disclose PHI for national security purposes, such as protecting the President of the United States or conducting intelligence operations.

m. Inmates. We may use or disclose your PHI if you are an inmate of a correctional facility and your physician created or received your PHI in the course of providing care to you.

n. Workers' Compensation. Your PHI may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally established programs.

3. **Written Authorization.** Any uses and/or disclosures of your PHI for purposes other than treatment, payment and health care operations, or as otherwise allowed or required by law as described above will be made ONLY with your written authorization. Any authorization you provide to us is effective for the period specified in the authorization unless you revoke the authorization in writing. Any written authorization may be revoked by you, at any time. Your revocation shall not apply to those uses and disclosures we made on your behalf pursuant to your authorization prior to the time we received your written revocation.

4. **Others Involved in Your Health Care or Payment for Your Care.** If you desire PHI to be disclosed to your family, a relative, a close friend or other person involved in your health care or who has responsibility for payment for your health care, it is our policy to require your written authorization, unless such authorization is clearly not required (i.e. a family member is with you).

5. **Your Rights.** Following is a statement of your legal rights with respect to your PHI and a brief description of how you may exercise these rights.

a. Right to Request Restrictions. You may ask us to restrict the use or disclosure of any part of your PHI. Your request must be in writing, addressed to our Privacy Officer and state the specific restriction requested and to whom you want the restriction to apply. We will consider your request but are not legally required to accept it in all instances.

b. Right to Receive Confidential Communications of PHI. You have the right to request that we send information to you at an alternative address or by alternate means (i.e. fax instead of regular mail). Your request must be in writing, addressed to our Privacy Officer, and state the accommodations you are requesting.

c. Right to Inspect and Copy. In most instances, you have the right to inspect or obtain copies of your PHI that we have; however, you must make the request for such inspection or copies in writing, addressed to our Privacy Officer. In certain situations, we may deny your request. If we deny your request, we will inform you in writing of our reason for the denial and explain your right to have the denial reviewed. There may be reasonable charges for copies made.

d. Right to Amend Your PHI. You may request an amendment of your PHI that we maintain. Such request must be in writing and addressed to our Privacy Officer. In certain cases, we may deny your request for an amendment.

e. Right to Receive an Accounting of Disclosures. You have the right to receive an accounting of certain disclosures we have made, if any, of your PHI. Your request for an accounting must be in writing, addressed to our Privacy Officer.

f. Right to Receive a Paper Copy. You have the right to receive a paper copy of this notice upon written request to our Privacy Officer.

6. **Breach Notification Requirement.** In the event of a breach of your PHI, we will provide you with notice of such breach as required by law.

7. **Complaints.** You may complain to us or to the Secretary of Health and Human Services if you believe we have violated your privacy rights. To complain to us, you may send our Privacy Officer a letter describing your concerns to the address found below. We will not retaliate against you for filing a complaint.

8. **Privacy Officer Contact Information.** If you have any questions about this Notice, you may contact our Privacy Officer by telephone or in writing at the address set forth below. If, however, you want to exercise any of your rights pursuant to this Notice of Privacy Practices or have a complaint, such action must be in writing and mailed to our Privacy Officer at the address set forth below.

VACCINATION SERVICES OF AMERICA, INC. d/b/a TOTALWELLNESS
ATTN: ALAN KOHLL, PRIVACY OFFICER
9320 H Court
Omaha, NE 68127
1-888-434-4358 x 102

EXHIBIT B

FORM OF ACKNOWLEDGEMENT

Vaccination Services of America, Inc. d/b/a TotalWellness
RECEIPT OF NOTICE OF PRIVACY PRACTICES

I acknowledge that I was offered a copy of the Vaccination Services of America, Inc. d/b/a TotalWellness Notice of Privacy Practices effective June 1, 2011.

Printed Name	Date
Signature of Patient/Parent/Legal Guardian	Relationship to Patient

Note: If signed by someone other than the patient, we need written proof of your authority.

DOCUMENTATION OF GOOD FAITH EFFORT

____ Attempted to distribute the Notice of Privacy Practices to the patient/parent/legal guardian, but the patient/parent/legal guardian declined to acknowledge the receipt of the Notice of Privacy Practices.

____ Patient/parent/legal guardian stated they had already received the Notice of Privacy Practices at another Vaccination Services of America, Inc. d/b/a TotalWellness service location.

____ The Notice of Privacy Practices was mailed to the patient/parent/legal guardian.

Witness	Date

[Note: This acknowledgement may be part of any other document that will be signed or initialed by a patient, however, there must be a separate place for the patient or either sign or initial the acknowledgement.]

EXHIBIT C

AUTHORIZATION FORM

AUTHORIZATION TO USE AND/OR DISCLOSE PROTECTED HEALTH INFORMATION

1) ☐ **Authorization for Release.** The undersigned hereby authorizes Vaccination Services of America, Inc. d/b/a TotalWellness and its employees to use and/or disclose to: _____

_____

_____

For the following purpose(s) (may state "per my request"): _____

_____

_____

___

The following health information:

☐ Entire medical record
☐ Entire medical record, excluding:
  ☐ Health information relating to testing, diagnosis, and/or treatment for HIV (AIDS virus)
  ☐ Health information relating to sexually transmitted diseases
  ☐ Mental health records
  ☐ Drug and/or alcohol abuse records
☐ Other (specify) _____

2) ☐ **Authorization to Release/Transfer.** The undersigned hereby authorizes _____ _____ to release the following health information to Vaccination Services of America, Inc. d/b/a TotalWellness and its employees for the purpose of continuation of my medical/surgical care:

☐ Entire medical record
☐ Entire medical record, excluding:
  ☐ Health information relating to testing, diagnosis, and/or treatment for HIV (AIDS virus)
  ☐ Health information relating to sexually transmitted diseases
  ☐ Mental health records
  ☐ Drug and/or alcohol abuse records
☐ Other (specify) _____

3) **Conditions.** We may not condition your right to receive health care services from us upon your signing this authorization. However, if the treatment to be provided is for research purposes, your failure to sign this authorization will prevent us from providing such treatment.

4) **Further Uses and Disclosures.** When we use or disclose your health information as you have instructed us in this authorization, we do not have the ability to monitor whether your health information may be further used or disclosed by such parties. In such a situation, your disclosed health information may no longer be protected by Federal and State privacy laws.

5) **Expiration.** This authorization shall expire upon the earlier of _____ or twelve (12) months from the date of this authorization. After the expiration date, we will need to obtain a new authorization from you if required by law.

6) **Revocation.** You have the right to revoke this authorization at any time by providing us with written notice by certified mail or hand delivery to the following address:

VACCINATION SERVICES OF AMERICA, INC. d/b/a TOTALWELLNESS
ATTN: ALAN KOHLL, PRIVACY OFFICER
9320 H Court
Omaha, NE 68127
1-888-434-4358 x 102

When we receive your revocation, we will immediately stop using and disclosing the health information you authorized us to use and disclose in this authorization form. Your revocation shall not apply to those uses and discloses we made on your behalf pursuant to this authorization prior to the time we received your written revocation.

7) **Marketing Authorization**. I understand that the Company will receive compensation for using/disclosing my PHI pursuant to this authorization. **[NOTE: include this provision only for marketing authorizations that involve direct or indirect remuneration to the Company from a third party.]**

PRINTED PATIENT NAME	PATIENT ACCOUNT NUMBER (IF KNOWN)
SIGNATURE OF PATIENT OR GUARDIAN	DATE

***NOTE: IF SIGNED BY SOMEONE OTHER THAN THE PATIENT, WE MUST HAVE WRITTEN PROOF OF HIS/HER AUTHORITY.**

EXHIBIT D

REQUEST FOR ALTERNATIVE COMMUNICATIONS

I request that the following alternative means and/or location be utilized for communication of confidential communications from Vaccination Services of America, Inc. d/b/a TotalWellness to me:

_____

_____

_____

_____ _____

Signature of Patient or Personal Representative Date

If signed by the patient's personal representative, explain your authority to act on behalf of the patient:

_____

EXHIBIT E
REQUEST FOR ACCESS

Patient Information:

Name: _____
Address: _____
Telephone Number: _____

I request access to the following records regarding my protected health information ("PHI") as more specifically described below:

_____

_____

Please provide me the information in the following format (i.e. hard copy, compact disk):

_____

Please provide me the requested information on or before this date: _____

I am requesting this information for the following purposes:

_____

_____

Contact information for the person requesting access is as follows:

Name:_____
Address:_____
Telephone Number:_____

I understand that Vaccination Services, Inc. d/b/a TotalWellness (the "Corporation") may provide me a summary or explanation of the PHI instead of providing access to the actual PHI, and this acknowledgement shall serve as my consent thereto. I also understand that the Corporation may charge a reasonable, cost-based fee for providing to me the requested PHI. Such fee includes only the costs of copying, postage, and preparation of an explanation or summary of the PHI, and does not include the cost associated with searching for and retrieving the records.

_____ _____
Signature of Patient or Personal Representative Date

If signed by the patient's personal representative, explain your authority to act on behalf of the patient:

_____

EXHIBIT F

REQUEST FOR AMENDMENT

Patient Information:

Name: _____
Address: _____
Telephone Number: _____

I request that the following records regarding my protected health information ("PHI") be amended as more specifically described below:

_____

_____

I am requesting this amendment for the following reasons:

_____

_____

The following persons/entities may have received information affected by this amendment and may have relied, or might rely in the future, on the information to the detriment of the Patient:

_____

_____

Contact information of person requesting amendment is as follows:

Name: _____
Address: _____
Telephone Number: _____

_____ _____
Signature of Patient or Personal Representative Date

If signed by the patient's personal representative, explain your authority to act on behalf of the patient:

_____

_____

EXHIBIT G

REQUEST FOR ACCOUNTING

Patient Information:

Name: _____
Address: _____
Telephone Number: _____

I am requesting an accounting regarding the uses/disclosures of the following protected health information ("PHI") as more specifically described below:

_____

_____

I am requesting this accounting for the following reasons:

_____

_____

_____

Contact information of person requesting accounting is as follows:

Name: _____
Address: _____
Telephone Number: _____

_____ _____
Signature of Patient or Personal Representative Date

If signed by the patient's personal representative, explain your authority to act on behalf of the patient:

_____

_____

EXHIBIT H

COMPLAINT FORM

Patient Information:

Name: _____
Address: _____
Telephone Number: _____

Please describe the type and nature of your complaint:

_____

_____

_____

Please provide the following specific information regarding your complaint, as applicable:

Corporation location: _____
Corporation employee: _____
Date incident occurred: _____

I am requesting this accounting for the following reasons:

_____

_____

_____

Contact information of person making complaint is as follows:

Name: _____
Address: _____
Telephone Number: _____

_____ _____
Signature of Patient or Personal Representative Date

If signed by the patient's personal representative, explain your authority to act on behalf of the patient:

_____

_____

EXHIBIT I

ELECTION AND CONSENT FOR COMMUNICATIONS FORM
OPTIONAL

I understand that Vaccination Services of America, Inc. d/b/a TotalWellness does not and cannot guarantee the confidentiality of any voicemail messages or email communications and will not be liable for improper disclosure of confidential information and/or breaches in information caused by me or a third party.

I hereby voluntarily request and consent to communicate with my physician and/or office personnel via the following communication methods.

1. Primary Number: _____ ___Home ___Work ___Mobile ___ Other ___ Doctor name and appointment information ___ Test results ___ Appointment instructions ___ Billing information	2. Secondary Number: _____ ___Home ___Work ___Mobile ___ Other ___ Doctor name and appointment information ___ Test results ___ Appointment instructions ___ Billing information
3. Tertiary Number: _____ ___Home ___Work ___Mobile ___ Other ___ Doctor name and appointment information ___ Test results ___ Appointment instructions ___ Billing information	4. Primary Email Address: _____ ___Home ___Work ___ Other ___ Appointment instructions

This is to authorize and request that you provide a copy of the results of my procedure(s) to the following:

1. _____

☐ Primary care doctor
☐ Other

2. _____

☐ Primary care doctor
☐ Other

_____ _____ _____
Patient Signature Patient Printed Name Date

If Patient is a Minor, has a Legal Guardian or a Power of Attorney exists:

_____ _____ _____
Responsible Party Signature Responsible Party Printed Name Date