HIPAA
Privacy & Security Plan

October 2016

HIPAA Privacy & Security Plan

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict USANotify Corporation ("USANotify" or "Company") abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Company and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Participant's medical record number
- Participant's demographic information (e.g. address, telephone number)
- Information doctors & other health care providers put in a participant's medical record
- Images of the participant
- Conversations a provider has about a participant's care or treatment with nurses and others
- Information about a participant in a provider's computer system or a health insurer's computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is the Company's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Plan. For purposes of this plan and the Company's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, interns, board members and other persons whose work performance is under the direct control of USANotify, whether or not they are paid by USANotify. The term "employee" or "staff member" includes all of these types of workers.

No third party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. USANotify reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

SECTION 1: Responsibilities as Covered Entity

I. Privacy Officer

The CEO will be the HIPAA Privacy Officer for USANotify. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at (732) 290-1900.

II. Incident Response Team

The Incident Response officer is comprised of Site Managers and additional members deemed appropriate on an ad hoc basis in the reasonable judgment of the Privacy Officer. In the event of a security incident results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team will take appropriate actions to prevent further inappropriate disclosures. In addition, HR may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required. If the Privacy Officer and Incident Response Team have not resolved the incident, the Privacy Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If participants need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

III. Workforce Training

It is the Company's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members that work with related products receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

IV. Safeguards

The Company has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements.

Technical Safeguards

The following technical safeguards have been put in place by USANotify to prevent unauthorized access, limit access to PHI, and log all access to systems and information:

- Firewalls in front of all servers
- Restricted user access to web portals by allowing specific IP Addresses only
- Log all user activity while they are using the systems
- Limit the number of login attempts
- Unique logins for each system user

- User permissions limit the capabilities of each user type
- Complex passwords required

Physical Safeguards

USANotify installs all equipment at Tier III data center facilities that are HIPAA compliant. Presently, all equipment is located at IO Data Center in Woodbridge, NJ. The following physical safeguards have been put in place by USANotify to prevent unauthorized access and limit access to PHI on all systems:

- Access card must have photo ID of authorized employee
- Access card must be registered with data center
- Employee must present and scan access card at manned gate
- Employee must scan access card and enter passcode at secure exterior door to facility
- Employee must show access card to manner foyer at facility
- Employee must scan access card and enter passcode at secure interior door to vestibule
- Employee must pass a retina scan in vestibule before accessing data center
- Employee must scan access card to enter data center pod
- Employee must know the 4 digit PIN to enter the cabinet
- Employee access is revoked after he/she leaves the company
- Any paper or digital media is locked in a filing cabinet at all times

Data Storage / Backup / Remote Access

Data storage is all kept at a Tier III data center facility. Data is routinely backed up using industry standards with onsite and offsite storage of media. USANotify currently utilizes technology that allows the IT team to quickly remove, disable and start staff member access to PHI.

Remote access to any equipment is allowed from authorized IP Addresses only and is controlled at the firewall and software levels. Furthermore, each user has a unique login and secure, encrypted password. In addition, all remote access activity is tracked and logged.

V. Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices that describes:

- Uses and disclosures of PHI that may be made by the Company
- Individual's rights
- Company's legal duties with respect to the PHI

The privacy notice will inform participants that the Company will have access to PHI. The privacy notice will also provide a description of the Company's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- On an ongoing basis & at the time of an individual's enrollment into the Company
- Within 60 days after a material change to the notice.
- Company will also provide notice of availability of the privacy notice at least once every 3 years.

VI. Complaints

The Privacy Officer will be the Company's contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Company's privacy procedures and for creating a system for handling such complaints. A copy of the complaint form shall be provided to any participant upon request.

VII. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

VIII. Mitigation of Inadvertent Disclosures of Protected Health Information

USANotify shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a Participant's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Company or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

IX. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

X. Plan Document

The Plan document includes provisions to describe the permitted and required uses and disclosures of PHI by USANotify. Specifically, the Plan document requires USANotify to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law
- ensure that any agents or subcontractors to whom it provides PHI received from the Company agree to the same restrictions and conditions that apply to USANotify
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures
- make PHI available to Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures

- make the Company's internal practices and records relating to the use and disclosure of PHI received by the Company available to the Department of Health and Human Services (DHHS) upon request

XI. Documentation

The Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

USANotify shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Incident Report

The Company has developed an Incident Report form. This form is used to document reports of privacy breaches that have been referred to the Privacy Officer from staff members who have reviewed or received the suspected incident.

After receiving the Incident Report form from staff members, the Privacy Officer classifies the incident and its severity and analyzes the situation. Documentation shall be retained by the Company for a minimum of six years from the date of the reported incident.

If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

XII. Electronic Health Records

Just like paper records, Electronic Health Records must comply with HIPAA, and other state and federal laws. Unlike paper records, electronic health records can be encrypted - using technology that makes them unreadable to anyone other than an authorized user - and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

XIII. Access Authorization

USANotify will grant access to PHI based on their job functions and responsibilities. USANotify asks clients to limit the data sensitivity transmitted to the maximum level required for the specific application. For example, appointment notifications should NOT include medical details of the appointment.

The Privacy Officer in collaboration with IT and senior management is responsible for the determination of which individuals require access to PHI and what level of access they require through discussions with the individual's manager and or department head.

The IT department will keep a record of authorized users and the rights that they have been granted with respect to PHI. IT keeps a comprehensive matrix of how and to who rights are granted. A summary of user rights can be found in the table below.

Job Title	**User Rights**
Front Desk / Reception	Access to demo system with no actual patient data
Technical Support	Restricted access to live systems from a specific IP Address. Using his/her own user login, support staff will have access to: - Client Appointment Details (for specified clients in one system) - Daily Appointment Reports - Patient Name and Phone Number - Provider Name and Location
Developer / Engineer	Restricted access to live systems from a specific IP Address. Using his/her own user login, development staff will have access to: - Client Appointment Details (for all clients in one system) - Daily Appointment Reports - Patient Name and Phone Number - Provider Name and Location
Accounting / Billing	Restricted access to live systems from a specific IP Address. Using his/her own user login, accounting staff will have access to: - Daily Billing Reports - Client billing information
Sales	Access to demo system with no actual patient data.
Senior Staff - Some Developers - Includes Executives	Restricted access to live systems from a specific IP Addresses. Using his/her own user login, senior staff will have access to: - Client Appointment Details (for all clients in all systems) - Daily Appointment Reports - Patient Name and Phone Number - Provider Name and Location (View/Add/Modify) - Billing Information for All Clients (View/Add/Modify) - User permissions (View/Add/Modify)

Clients	Restricted access to his/her own live system from a specific IP Addresses. Using his/her own user login, clients will have access to: - Client Appointment Details (for all sub-clients) - Daily Appointment Reports - Patient Name and Phone Number - Provider Name and Location (View/Add/Modify) - Billing Information for All Sub-Clients (View/Add/Modify) - User permissions for sub-clients
Partners	Restricted access to his/her own clients' live systems from a specific IP Addresses. Using his/her own user login, partners will have access to: - Client Appointment Details (for all clients in all clients' systems) - Daily Appointment Reports - Patient Name and Phone Number - Provider Name and Location (View/Add/Modify) - Billing Information for All Sub-Clients (View/Add/Modify) - User permissions for sub-clients

SECTION 2: Use and Disclosure of PHI

I. Use and Disclosure Defined

The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company, or by a Business Associate of the Company.
- *Disclosure.* For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within USANotify with a business need to know PHI.

II. Access to PHI Is Limited to Certain Employees

All staff members that perform Participant functions directly on behalf of the Company will have access to PHI as determined by their department and job description and as granted by IT.

These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through our information systems any information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes, even if written or oral participant authorization has been given.

In the very rare circumstance when a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she should immediately report the situation to his/her manager who will determine whether to assign a different staff member to complete the task involving the specific Participant.

Your access to your own PHI must be based on the same procedures available to other participants not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any Participant would have to.

III. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IV. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Company's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- about victims-of abuse, neglect or domestic violence
- for judicial and administrative proceedings
- for law enforcement purposes
- to avert a serious threat to health or safety
- for specialized government functions
- that relate to workers' compensation programs

V. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual
- uses or disclosures made pursuant to a valid authorization
- disclosures made to the Department of Labor
- uses or disclosures required by law
- uses or disclosures required to comply with HIPAA

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

VI. Disclosures of PHI to Business Associates

With the approval of the Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the Company's business associates and allow the Company's business associates to create or receive PHI on its behalf. However, prior to doing so, the Company must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.)

- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Examples of Business Associates are:

- A third party administrator that assists the Company in any way
- A CPA firm whose accounting services involves access to protected health information.
- An attorney whose legal services involve access to protected health information.

VII. Disclosures of De-Identified Information

The Company may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

18 specific elements listed below - relating to the participant, employee, relatives, or employer - must be removed, and you must ascertain there is no other available information that could be used alone or in combination to identify an individual.

1. Names
2. Geographic subdivisions smaller than a state
3. All elements of dates (except year) related to an individual - including dates of admission, discharge, birth, death - and for persons > 89 years of age, the year of birth cannot be used.
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social Security Number
8. Medical Record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos, and comparable images
18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual AND this person must document the methods and justification for this determination.

VIII. Removing PHI from Company Premises

When USANotify deems it necessary for an employee to work from a location other than one of our sites, PHI may be accessed and/or removed under the following circumstances:

1. Before removing PHI from USANotify for company business you must receive the approval from management.
2. USANotify will only allow the paper (participant records, reports) removal of PHI when transported in a secure lock box and when approved by management
3. Remote access will only given to the IP address specified by the user. Any files saved on the remote computers are saved to the network and are therefore secure.
4. The electronic removal of PHI (using flash drives) for the purposes of working from a remote setting may be approved in advance by management only. In the very rare circumstance that it becomes necessary, the PHI should be rigorously safeguarded physically as well as electronically, including *employee-performed* encryption of all files. Most flash drives have the capability to assign a password.
5. The following safeguards are required of all employees when working from a remote site:

    a. When outside the facility, only work on health information in a **secure private environment.**
    b. Keep the information with you **at all times** while in transit.
    c. Do not permit others to have access to the information
    d. Never email participant information.
    e. Don't save participant information to your home computer
    f. Do not print records of any type.
    g. Do not record login information on or near the computer.
    h. Return all information the next business day or as soon as required.

USANotify will immediately investigate any incident that involves the loss or theft of PHI that was taken off-site.

IX. Faxing PHI

Each fax should be accompanied by a USANotify fax cover sheet. Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:

Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. Document the incident on an Incident Report Form and notify the HIPAA Privacy Officer at (732) 290-1900. Verify the fax number with the recipient before attempting to fax the information again.

SECTION 3: Participant Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Company or its business associates maintains. HIPAA also provides that participants may request to have their PHI amended. The Company will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations
- to individuals about their own PHI
- incident to an otherwise permitted use or disclosure or pursuant to an authorization
- for purposes of creation of a facility directory or to persons involved in the participant's care or other notification purposes
- as part of a limited data set
- for other national security or law enforcement purposes.

The Company shall respond to an accounting request within 60 days. If the Company is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings. The Privacy Officer is responsible for responding to a request for Accounting.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of USANotify, the requests are reasonable.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Company’s policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Privacy Officer is charged with responsibility for processing requests for restrictions.

V. When a Participant Requests a Copy of his/her Record

A participant can request a copy of his/her medical record by completing a Request for Accessing/Inspecting/Copying Health Information form and submitting it to the Department that maintains the information being requested. The Department in collaboration with the Privacy Officer must process and respond to the request.

Participants can receive this form from Patient Services or by going directly to the department that maintains their records.

VI. Acceptable Methods of Verification of Identity for Release of PHI:

When the Requestor is the Participant

The Company will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI.

1. **If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the Participants record.
2. **If the request is made over the telephone**, verification will be accomplished by requesting identifying information such as social security number, birth date, and medical record number and confirming that this information matches what is in the participant's record. Or, verification will occur through a callback process using phone numbers documented in the participant record to validate the caller's identity.
3. **If the request is made in writing,** verification will be accomplished by requesting a photocopy of photo identification. In addition, USANotify will need to verify the validity of the written request by contacting the participant by telephone.

V1I. When the requestor is the Participants Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the participant's profile as the participant's legally authorized representative. Or, if there is no person listed in the medical record as the participant's legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the participant and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the Participants record.

VIII. Other Methods

The Company may use any other method of verification that, in the Company's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

1. Requesting to see a photo ID
2. Requesting a copy of a power of attorney
3. Confirming personal information with the requestor such as date of birth, policy number or social security number
4. Questioning a child's caretaker to establish the relationship with the child
5. Calling the requestor back through a main organization switchboard rather than a direct number

PHI Breach Reporting

The purpose of this section is to address the Company's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Company. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members are required to verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a participant PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the manager determines that further review is required, the manager and staff member will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation. In all cases and Incident Report must be filled out and submitted to the appropriate reviewer.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is <u>not</u> considered part of the participant's health record.

If the participant is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the participant should be informed. If the participant is aware of a privacy incident, the Privacy Officer shall contact the participant within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer, but resulting communications with the participant must be documented in the incident report. In addition, any privacy incident that includes a disclosure for which an accounting is required must be documented and entered into accounting.

Staff who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

I. Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals if necessary and in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- *Individual Notice*

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by

first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- *Media Notice*

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- *Notice to the Secretary*

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- *Notification by a Business Associate*

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

II. Complaint/Concerns Reporting

Concerns about the Company's privacy practices may arise in a variety of contexts and may be received by many different persons at the Company. It is important that the Company responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she should ask the complainant whether or not the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

1. Participant's complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member the person receiving the complaint will:

a. In response to a Telephone Call or In-Person Request to File a Complaint – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Offer to forward a copy of the complaint form to the complainant.
b. In response to a Letter or Email (print out) – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Attach the written complaint to the complaint form.
c. In response to an Anonymous Complaint– Complete the Privacy Complaint Form based on the information provided and immediately forward to the Privacy Officer. When possible, explain to the complainant that the Company has an obligation to follow up on complaints whether or not they are anonymously filed.

2. **Staff Members** – Call the Privacy Officer at (732) 290-1900. Staff members may also complete the Privacy Complaint Form and forward to the Privacy Officer. Staff members can also fill out the complaint form and put it in the Privacy Officers mail box located at 1230 Hwy 34, Aberdeen, NJ 07747. Upon receipt of a complaint, the Privacy Officer will initiate primary investigation.

a. **Initial review** – All complaints will be initially reviewed by the Privacy Officer or his/her designee to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of this finding within 60 days. All documentation will be maintained as prescribed in this policy.
b. **Complaints requiring further review** – If there is a legitimate allegation, the Privacy Officer or his/her designee will conduct a detailed investigation by reviewing the covered University unit practices, contacting employees, students, or volunteers as needed, working with the Security Officer (as applicable), and utilizing other University resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of the finding within 60 days.
c. **60-day time frame –** In the event that this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.
d. **Outcome of Investigation -** The purpose of the investigation is to determine the compliance of the Company's policies and procedures implementing the privacy standards mandated by HIPAA. The Company will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of the Company's policies and procedures or HIPAA's privacy

requirements by the Company or any of its Business Associates. In the event that disciplinary action is recommended, the Privacy Officer or his/her designee will coordinate any action with management.

e. **Documentation -** All complaints sent to the Privacy Officer shall be documented in a format that includes all of the information contained on the Privacy Complaint Form. The Privacy Officer will maintain all completed complaints' documentation for six years from the initial date of the complaint.

III. Non-Retaliation

The Company shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.