HIPAA Policy and Training Manual

March 2015

2501 Cottontail Lane, Suite 101 • Somerset, NJ 08873
1-888-906-7141

HIPAA Policy and Training Manual

Table of Contents

OVERVIEW 1
- HIPPA and the HITECH Act 1
- Definition of Terms 1

INDIVIDUAL RIGHTS UNDER HIPAA 2

OUR ORGANIZATION'S RESPONSE TO HIPAA 4
- Compliance Officer 4
- Workforce Training and Oversight 4
- Patient Notification and Acknowledgement 4
- Structural Safeguards 5

USE, DISCLOSURE AND PRECAUTION GUIDELINES 6
- Treatment, Payment, and Health Care Operations 6
- Fax and E-mail Communications 8
- Level Necessary Policy 9
- Family Members, Personal Representatives and Power of Attorney 9
- Business Associates 11
  - Business Associate Agreements 12
  - Instances When Business Associate Agreements are NOT Needed 12
- Public Health Provision 13
- Workers' Compensation and Judicial/Administrative Proceedings 14

MARKETING COMMUNICATIONS UNDER HIPAA 15
- Written Authorization 15
- Use in Core Health Care Functions 15
- Financial Remuneration Rules 15

ENFORCEMENT AND VIOLATIONS 16
- Questions and Complaints 16
- Violations 16
- Breach Notifications 16
- Sanctions for Failing to Comply 17

Appendix - Forms

Name	Form #
Notice of Privacy Practices	0008Gen
Acknowledgment of Receipt of Privacy Practices Notice	0007-4Gen
Authorization to Release Health Information	0015Gen
Request for Restriction of Use and Disclosure of Protected Health Information	0021Gen
HIPAA Privacy Violation Complaint Form	0024Gen
Business Associate Agreement	0026Gen

OVERVIEW

HIPAA is the acronym for the *Health Insurance Portability and Accountability Act* of 1996. The purpose of this federal law was to improve portability of health insurance coverage, reduce healthcare fraud and abuse, and to protect the privacy of personal health records.

The federal agency responsible for putting HIPPA into action is the U.S. Department of Health and Human Services (DHHS). DHHS administers HIPAA by publishing federal regulations (also known as *rules*) and setting deadlines for organizations to comply. DHHS has put in effect several sets of regulations since HIPPA first went into effect.

In January 2013, DHHS enacted a significant update called the HIPPA Omnibus Rule (also referred to as the HIPAA *Mega Rule*). It marked the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. This *Mega Rule* provided the public with increased control over personal health information and fortified privacy, security, breach notification and enforcement rules.

HIPPA and the HITECH Act

The HIPPA Omnibus Rule reflects significant modifications that were mandated by the HITECH Act (Health Information Technology for Economic and Clinical Health). HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contained incentives related to health care information technology in general and contained specific incentives designed to accelerate the adoption of electronic health record systems among providers.

As healthcare providers move toward exchanging large amounts of health information electronically, the HITECH Act put in place safeguards to ensure that individual information remains private and secure.

Definition of Terms

Covered Entities: HIPAA rules apply only to individuals, organizations and agencies that meet HIPAA's definition of a *covered entity*. Covered entities are defined in the HIPAA rules as the following:

- **Health Care Providers** –includes hearing health care.
- **Health Plans** –group health plans, certain long-term care plans, insurers, and HMOs.
- **Health Care Clearinghouses** –independent organizations that receive insurance claims from health care providers and redistributes the claims electronically to various insurance carriers.

Personal Health Information (PHI): PHI includes all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity, including oral communications. PHI includes demographic information

collected from an individual that identifies, or can reasonably be used to identify, an individual. Examples of PHI are as follows (not an exhaustive list):

- Name
- Address
- Dates (such as birthday, date of service, etc.)
- Phone/fax number
- E-mail address
- Social security number
- Medical record number
- Insurance information
- Account number
- License number
- Device serial number

The HIPAA Privacy Rule: Refers to a set of national standards that became finalized law in 2003 and received a major enhancement in 2013 through the HIPPA Omnibus Rule. The Privacy Rule protects the privacy of patients' medical records and other health information maintained by covered entities.

INDIVIDUAL RIGHTS UNDER HIPAA

The HIPAA Privacy Rule sets standards with respect to the rights of individuals to their health information, procedures for exercising those rights, and the authorized and required uses and disclosures of such information. Individuals have the right to:

Receive a Copy of a Covered Entity's Notice of Privacy Practices. The written notice must provide a clear, user-friendly explanation of the individual's rights with respect to his or her personal health information and the covered entity's privacy practices.

Request Restrictions on PHI. Individuals have the right to request restrictions regarding the use and disclosure of their PHI for treatment, payment, and healthcare operations. The law also grants individuals the right to request restrictions for other disclosures, such as those made to family members. Covered entities are NOT required to agree to the restrictions requested.

The HIPAA Omnibus Rule and HITECH Act take the request for restrictions one step further, and require that "a covered entity must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if the disclosure is for the purposes of carrying out payment or health care operations and not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full."

Inspect and/or Receive A Copy of His or Her PHI. The Privacy Rule (with few exceptions) gives individuals the right to inspect, review, and receive a copy of his or her PHI (for example, medical and billing records). If an individual requests a copy of his or her PHI, the covered entity is allowed to charge a reasonable fee for the cost of supplies, labor, and postage. Individuals requesting copies from our company may be charged $14 for 1-10 pages and $0.50 per page for pages 11-40, and $0.33 per page for

every additional page. Actual postage costs will be added if the individual would like the information mailed to him or her. If the individual requests an alternative format, we will charge a cost-based fee for providing him or her health information in that format. If the individual prefers, we will prepare a summary or an explanation of his or her health information for a fee. Individuals may contact us our Compliance Officer for a full explanation of our fee structure.

The HITECH-HIPAA Omnibus Rule expands this right, giving individuals the right to access their own e-health record in an electronic format and to direct the covered entity to send the e-health record directly to a third party. The covered entity may only charge for labor and electronic transfer costs.

Request Corrections to PHI. If an individual thinks the information in his or her medical or billing record is incorrect, he or she can request that our company amend the record. We are required to respond to requests and make changes to inaccurate or incomplete information. This rule also applies to a person authorized to act on behalf of the individual in making health care related decisions such as the individual's personal representative.

Obtain an Accounting of Disclosures. Under HIPAA, covered entities are required to track disclosures of PHI. The purpose of tracking disclosures is to give an individual the right to receive a written account of when and with whom his or her information has been shared within the six years prior to the date of their request. If files are maintained electronically, the tracking period is limited to disclosures made within a three-year period. When requested, the covered entity must either:

- Provide an individual with an accounting of such disclosures made by the covered entity and all of its business associates.
- Provide an individual with an accounting of the disclosures made by the covered entity and a list of business associates, including their contact information, and who will be responsible for providing an accounting of such disclosures upon request.

Not all disclosures require tracking or need to be accounted for upon request by an individual. We are NOT required to track disclosures made for:

- Treatment, payment, and healthcare operation purposes.
- To the individual.
- To persons involved in the individual's care.
- National security or intelligence purposes or to correctional institutions or law enforcement officials.

File a Complaint. A patient has the right to complain if he or she feels that anyone in our company used or disclosed his or her PHI inappropriately. Patients can make us aware of concerns by contacting our Compliance Officer or by submitting a written complaint to the US Department of Health and Human Services. We support our patients' right to privacy of PHI and will NOT retaliate in any way if they choose to file a complaint.

Receive Notice of a Breach. Affected individuals have the right to be notified if there has been an unauthorized acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by the Privacy Rule. He or she must receive notification without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach.

OUR ORGANIZATION'S RESPONSE TO HIPAA

We have had policies and practices in place for many years surrounding confidentiality of information. As HIPAA regulations evolve and update we are required and committed to enhancing and changing our policies and practice as necessary. This guide describes our current policies and procedures.

Compliance Officer

Due to the size and multi-office nature of our company there is a need to create a standardized and uniform approach to the handling of PHI. To meet this need, one individual fulfills the role of our company's Compliance Officer. The Compliance Officer serves under the direction of the Chief Executive Office (CEO) and is responsible for the development, implementation and maintenance of our privacy and compliance-related activities. The Compliance Officer ensures that PHI is protected from unauthorized access, yet remains accessible to individuals and to staff carrying out care and treatment. Contact information for our Compliance Officer is as follows:

Compliance Officer: Steve W. Barlow
Phone: 1-888-906-7141
Address: 2501 Cottontail Lane, Ste. 101
Somerset, NJ 08873

Workforce Training and Oversight

It is our company's policy to train all members of our workforce who have access to PHI on our privacy policies and procedures. Employees are required to complete an online HIPAA and HITECH training course to gain a full understanding of the general HIPAA privacy procedures, read and follow this training manual, and adhere to any other requirements that may be dictated directly by HIPAA.

Whenever a privacy incident has occurred, the Compliance Officer, in collaboration with management, will evaluate the occurrence to determine whether additional staff training is in order. Any training developed to respond to the incident will be reviewed by the Compliance Officer to ensure it adequately addresses the incident and reinforces the company's privacy policies and procedures.

Patient Notification and Acknowledgement

All of our patients receive written notice of our privacy practices. In most cases the notice will be given to the patient on his or her first visit to us. The notice describes how we use

and disclose patient PHI, the patient's right to access to his or her PHI, and our legal duties concerning PHI. Patient notification is accomplished as follows:

Paper Notification and Acknowledgment: We offer our patients a handout that gives notice of our privacy practices. HIPAA law requires we ask each patient to state in writing that they have received the notice. The law does NOT require patients to sign the acknowledgment of receipt of privacy practices. If a patient refuses to sign the acknowledgement we are required to keep a record that we made a good faith effort to obtain the patient's signature. Space to record the patient's acknowledgment of receipt of our Privacy Practices Notice is part of our intake form or can be recorded on a standalone form.

Electronic Notification and Acknowledgment: When a patient has received electronic notification of our privacy practices, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice. A provider who gives paper notice to a patient during a face-to-face encounter may obtain an electronic acknowledgment from the individual, provided that the individual's acknowledgment is in writing. Thus, a receptionist's notation in the provider's computer system of the individual's receipt of the notice would NOT be considered a valid written acknowledgment.

Posted Notification: All offices or other physical sites where we provide care directly to individuals are required to post a notice of privacy practices in its entirety. The posted notice must be in a clear and prominent location. HIPAA rules do not prescribe any specific format for the posted notice, just that it include the same information that is distributed directly to the individual. HIPAA rules allow us the discretion to design the posted notice in a manner that works best for each facility, which may be to simply post a copy of the notice that is distributed directly to individuals. However, in most situations our offices will use a 1-sided, enlarged, framed version of our handout to satisfy this rule.

Intimidation or Waiver Prohibited: 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.

Structural Safeguards

The HIPAA Privacy Rule is NOT intended to prohibit providers from talking to each other or to their patients; nor are we required to retrofit offices to provide private rooms or soundproof walls to avoid any possibility that a conversation is overheard. Provisions of this Rule do require us to take reasonable steps such as the following to ensure privacy and security:

- Patient Care Coordinators should ask waiting customers to stand a few feet back from a counter used for patient counseling, check-ins or payments.

- Patient Care Coordinators should make every effort to cover up patient records at the front desk while other patients are in the waiting area.
- Health Care Practitioners should use a private office to discuss the outcome of a hearing test, to counsel, dispense, and otherwise treat patients when available and practicable.
- Areas that house patient files should be supervised or locked.
- Office doors should be checked to ensure that they are locked and patient records are put away before employees leave areas that house patient files unattended.
- Patient records containing PHI should be secured so that they are not readily available to those who do not need them.

USE, DISCLOSURE AND PRECAUTION GUIDELINES

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally.

For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices. Rather, the Privacy Rule permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

HIPAA's privacy regulations permit covered entities to use and disclose PHI *WITHOUT* first obtaining written authorization from the patient as follows:

- As necessary to carry out medical treatment, payment or health care operations.
- To the patient.
- To a patient's family member or personal representative. (Certain restrictions apply. See section on Family Members for details.)
- Pursuant to, and in compliance with, the patient's authorization.
- In certain other instances without the individual's consent, authorization or opportunity to object.

Treatment, Payment, and Health Care Operations

To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for treatment, payment and health care

operations activities. (Certain exceptions apply in instances where the PHI in question is psychotherapy notes.) Examples of this type of permitted use are as follows:

Scheduling and Reports: Health care providers, such as a specialist or hospital to whom a patient is referred for the first time, are permitted to use an individual's PHI to set up appointments, schedule surgery, or other procedures without first obtaining the patient's written consent.

Consultations Between Providers: Consultation about a patient's condition is permitted between health care providers without the obtaining a patient's written authorization. In addition, a health care provider (or other covered entity) is expressly permitted to disclose PHI about an individual to a health care provider for that provider's treatment of the individual.

Confidential Conversations: The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and/or to their patients even if there is a possibility that the conversation could be overheard. The Privacy Rule recognizes that overheard communications in some settings may be unavoidable and allows for some incidental disclosures. The following examples of confidential communication are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Orally coordinating services at the front desk.
- Discussing a patient's condition over the phone with the patient, a provider, or a family member.
- Discussing diagnostic hearing test results with a patient or other provider in a joint treatment area while another patient is present.
- Discussing a patient's condition with a dispenser trainee as part of their training.

In the examples above, reasonable precautions may include using lowered voices or talking apart from others. However, where a patient is hearing impaired, such precautions may not be practicable. We are free to engage in communications as required for quick, effective, and high quality health care.

Sign-in Sheets and Calling Out Names: HIPAA rules allow us to use patient sign-in sheets or call out patient names in waiting rooms so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice; for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. Reasonable safeguards include the following:

- Sign in sheets may only include the minimum amount of PHI necessary to call the patient and must specifically exclude diagnostic information. For example, the sign-

in sheet may NOT display medical information that is not necessary for the purpose of signing in (e.g., the specific problem for which the patient is being seen).

- Computer screens with patient information must be kept secure and turned away from the patients.
- Patients are not allowed to go behind a desk where the computer screen would be visible.
- When speaking to patients in the waiting room, staff will encourage patients to come to the front desk to receive further instructions in a more confidential manner.

Patient Charts: The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it dictate the specific measures that must be applied to protect an individual's privacy while engaging in these practices. Reasonable steps we take when using patient charts are as follows:

- Staff using patient charts outside of exam/consultation rooms will make sure the charts are not accessible to other patients or non-employees.
- When patient charts are in wall holders, identifying information must face the wall or otherwise be covered, rather than having health information about the patient visible to anyone who walks by.

Medical Trainees: The definition of health care operations in the Privacy Rule provides for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers. Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit trainees access to patients' medical information, including entire medical records. Hearing Care Practitioner trainees are allowed to access patient medical information as part of their training.

Fax and E-mail Communications

The HIPAA Privacy Rule permits us to communicate PHI to another health care provider for treatment purposes by way of fax, e-mail or other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed.

Fax Safeguards

- Sender must verify that the fax number to be used is in fact the correct one for the health care provider.
- Fax machine must be in a secure location to prevent unauthorized access to the information.
- Outgoing facsimile transmissions must contain the following disclaimer on the fax cover page:

Confidentiality Notice: This message is intended only for the use of the individual or entity to which it is addressed and may contain Protected Healthcare Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error, please immediately notify the sender via telephone or return fax.

E-mail Safeguards

- Sender must verify that the e-mail is addressed only to the intended recipient, the e-mail address is spelled correctly and that the content is in full compliance with the HIPAA Policy and Training Manual.
- If the e-mail contains clinically relevant information, the sender must print a copy of it and place it in the patient's medical records.
- The following e-mail disclaimer must be added to every outgoing e-mail:

  Confidentiality Notice: This e-mail is intended only for the use of the individual or entity to which it is addressed and may contain Protected Healthcare Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this e-mail in error, please immediately notify the sender via telephone or return e-mail.

Level Necessary Policy

It is our company's policy to allow our Health Care Practitioners, Patient Care Coordinators, as well as management to have access to the level of PHI (minimum necessary or entire record) as is required to fulfill proper treatment, payment, and operation functions.

Minimum Necessary: When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The determination of what constitutes minimum necessary data is left to the judgment of the covered entity.

Entire Records: The Privacy Rule does NOT prohibit the use, disclosure, or request of an entire medical record. A covered entity may use, disclose, or request an entire medical record without a case-by-case justification if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

Family Members, Personal Representatives and Power of Attorney

HIPAA rules do NOT require covered entities to obtain written permission before sharing or discussing PHI with a patient's family members, friends, or others involved in a patient care or payment for care. However, a provider may prefer or require that patients give written permission. If the patient is present and has the capacity to make health care

decisions, a health care provider may discuss the patient's health information with others if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Similarly, information relating to an individual's location, general condition, or death may be disclosed or used to notify a family member, personal representative or other person responsible for care of the individual.

Obtaining PHI of a Deceased Family Member: The HIPAA Privacy Rule recognizes that a deceased individual's PHI may be relevant to a family member's health care. The Rule allows covered entities to release the PHI of a deceased relative to a surviving family member under the following circumstances:

- **PHI is to be Used For Treatment Purposes:** Using PHI from one individual in the treatment of another individual does not require an authorization. Thus, a covered entity may disclose a decedent's PHI, without authorization, to the health care provider who is treating the surviving relative.
- **Authorized Disclosure:** A covered entity must treat a deceased individual's legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual or his estate, as a personal representative with respect to PHI relevant to such representation. Therefore, if it is within the scope of such personal representative's authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.

Parents and Children: The Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with state or other law. However, there are situations when the parent would NOT be the minor's personal representative under the Privacy Rule. These situations are as follows:

- When the minor is the one who consents to care and the consent of the parent is not required under state or other applicable law.
- When the minor obtains care at the direction of a court or a person appointed by the court.
- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

Even in these exceptional situations, the parent may have access to the medical records of the minor when state or other applicable law requires or permits such parental access. Parental access would be denied when state or other law prohibits such access.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a

provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

Power of Attorney: Nothing in the Privacy Rule changes the way in which an individual grants another person power of attorney for health care decisions. State law (or other law) regarding health care powers of attorney continue to apply. The intent of the provisions regarding personal representatives was to complement, not interfere with or change, current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions that give others the ability to exercise the rights of, or make treatment decisions related to, an individual. The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under other law, the ability to exercise the rights of that individual with respect to health information.

Non-applicable Power of Attorney: Power of attorney given to a person for purposes other than health care, such as a power of attorney to close on real estate, does NOT authorize the holder to exercise the individual's rights under the HIPAA Privacy Rule.

Further, a covered entity does not have to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

Except with respect to decedents, a covered entity must treat a personal representative as the individual only when that person has authority under other law to act on the individual's behalf on matters related to health care.

Business Associates

The HIPAA Privacy Rule applies only to covered entities (health plans, health care clearinghouses, and health care providers). However, most covered entities do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses, which HIPAA refers to as *business associates*.

The Privacy Rule allows covered entities to disclose PHI to business associates if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Covered entities may disclose PHI to an entity in its role as a business associate only to help the covered entity carry out its health care functions—not for the Business

Associate's independent use or purposes, except as needed for the proper management and administration of the Business Associate.

Examples of our business associates receiving PHI include hearing aid manufacturers, insurance companies, and nursing facilities. When disclosing PHI to business associates it is our policy to

- Make reasonable efforts to limit PHI disclosures to the minimum necessary to provide treatment, receive payment, or conduct health care operations.
- If there is any indication that a business associate receiving PHI is, or may be using, the information in a manner that is inconsistent with the services requested, immediately notify the Compliance Officer to investigate the concern.
- Employees are prohibited from selling or providing PHI to business associates for marketing purposes as defined by HIPAA (see Marketing Communications Under HIPAA section for details).

Business Associate Agreements

The HIPAA Privacy Rule does NOT hold covered entities liable for, or require them to monitor, the actions of its business associates. It requires we enter into written contracts or other arrangements with business associates that protect the privacy of PHI. We are NOT required to monitor or oversee the extent to which the business associate abides by the privacy requirements of the contract.

However, if a covered entity finds out about a material breach or violation of the contract by the Business Associate, it must take reasonable steps to cure the breach or end the violation. If unsuccessful, the contract with the business associate must be terminated. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights.

With respect to business associates, the HIPAA Privacy Rule considers a covered entity out of compliance if it fails to take the steps described above. If a covered entity's out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of PHI to the business associate are not permitted.

Instances When Business Associate Agreements are NOT Needed

Treatment Purposes: Health care providers often have business associate relationships with other health care providers. The HIPAA Privacy Rule explicitly excludes them from needing a business associate agreement because their disclosures are made for treatment purposes. Therefore, any covered health care provider (or other covered entity) may share PHI with a health care provider for treatment purposes *WITHOUT* a business associate contract.

However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract

WOULD BE REQUIRED before the hospital could allow the health care provider access to patient health information.

Inadvertent Contact: A business associate contract is *NOT* required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all. For example, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of PHI, and any disclosure of PHI to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule.

Health Providers And Health Plan or Payer: Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity's acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "Business Associate."

Public Health Provision

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to an individual's PHI to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose PHI without authorization for specified public health purposes.

Please Note: The Privacy Rule's public health provision ***permits***, but ***does not require*** covered entities to make the public health disclosures described above. This provision is intended to allow covered entities to continue current voluntary reporting practices that are critically important to public health and safety. The Rule also permits covered entities to disclose PHI when state or other law requires covered entities to make disclosures for public health purposes.

Disclosure of Findings to Employers. The public health provision permits covered health care providers to disclose an individual's PHI to the individual's employer *WITHOUT* authorization in very limited circumstances. These circumstances include:

- The covered health care provider has provided the health care service to the

individual at the request of the individual's employer or as a member of the employer's workforce.

- The health care service provided relates to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury.
- The employer has a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes described above. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the PHI the employer needs to meet such legal obligation may be disclosed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there).

Workers' Compensation and Judicial/Administrative Proceedings

Workers' Compensation: The HIPAA Privacy Rule does NOT apply to entities that are workers' compensation insurers, workers' compensation administrative agencies, or employers, except to the extent they may otherwise be covered entities. However, these entities need access to the health information of individuals who are injured on the job or who have a work-related illness to process or adjudicate claims, or to coordinate care under workers' compensation systems. Generally, this health information is obtained from health care providers who treat these individuals and whom the Privacy Rule may cover.

The Privacy Rule recognizes the legitimate needs of the workers' compensation systems to have access to PHI as authorized by state or other law. Due to the significant variability among state laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes without the individual's authorization to the extent disclosure is required by state or other law. The disclosure must comply with and be limited to what the law requires. Disclosure is permitted if an individual has provided his or her authorization for the release of the information to the entity. Individuals do NOT have a right under the Privacy Rule to request that a covered entity restrict a disclosure of his or her PHI if it is required by law and necessary to comply with workers' compensation or a similar law.

Judicial/Administrative Proceedings: The Privacy Rule generally permits covered entities to disclose an individual's PHI without first obtaining the individual's consent or offering him or her the opportunity to agree or object in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process.

MARKETING COMMUNICATIONS UNDER HIPAA

Marketing generally means a communication about a product or service that encourages the individual to purchase or use the product or service. The HIPAA Privacy Rule gives individuals important controls over whether and how their PHI is used and disclosed for marketing purposes.

Written Authorization

With limited exceptions, the HIPAA Privacy Rule requires an individual's written authorization before use or disclosure of his or her PHI can be made for marketing. Examples of marketing activities prohibited without written authorization from the individual would be to

- Provide names of hearing impaired patients to assistive listening device manufacturers or magazines.
- Supply patient lists to nursing facilities for the nursing facilities' promotions without the patient's authorization.

Use in Core Health Care Functions

So as not to interfere with core health care functions, the Privacy Rule has always distinguished marketing communications about goods and services that are essential for quality health care from other types of marketing. However, passage of the HITECH Act and HIPPA Omnibus Rule have tightened certain marketing communications activities related to core health care functions that were previously permitted without authorization. Types of communications permitted without written authorization from the individual are as follows:

- Case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care to the individual.
- Communications to describe a health-related product or service (or payment for such product or service) that is provided by, included or enhances an individuals plan of benefits.
- Contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

If the covered health care provider receives financial remuneration in exchange for any of the above activities, the communication will be *EXCLUDED* from the definition of core health functions and the communication is prohibited without first receiving written authorization from the individual.

Financial Remuneration Rules

Under HIPAA's Privacy Rule, merely having a "financial relationship" between the third party and the covered entity is not sufficient by itself to implicate the rule. Instead, under HIPAA's Privacy Rule the purpose of the financial remuneration must specifically be to

pay the covered entity to make a communication that encourages individuals to purchase or use the third party's product or service. For example, a covered entity would not need to obtain authorizations prior to sending communications encouraging individuals to participate in the covered entity's disease management program, even if a third party provided financial remuneration to the covered entity to implement the program, as long as the communications were directing individuals to the covered entity's program, and not the third party's product or service.

ENFORCEMENT AND VIOLATIONS

Questions and Complaints

The Compliance Officer is responsible for creating a process for individuals to inquire about our company's privacy practices, lodge complaints and for handling such complaints.

Violations

The Incident Response Team is comprised of the CIO (chief information officer), COO (chief operations officer), 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 that results in a wrongful disclosure of PHI, the Compliance Officer, in conjunction with the Incident Response Team will take appropriate actions to prevent further inappropriate disclosures. In addition, Human Resources and Legal may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required.

If the Compliance Officer and Incident Response Team have not resolved the incident, the Compliance 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 Compliance Officer will send PHI theft/loss disclosure letters to all possible affected individuals.

Breach Notifications

Under The HITECH Act covered entities and business associates are required to notify affected individuals if there is an unauthorized acquisition, access, use, or disclosure of unsecured PHI, subject to certain limited exceptions. PHI is considered unsecured unless it is encrypted or destroyed through the use of methodologies and technologies specifically approved in guidance issued by the US Department of Health and Human Services (DHHS).

If unsecured PHI has been breached, affected individuals must be notified by first-class mail or by e-mail if the individual specifies e-mail. If contact information for fewer than 10 individuals is insufficient or out-of-date, notice of the breach may be accomplished

by an alternative form of written notice such as by telephone or other means. If a posted notice on the homepage of our website (or through a hyperlink on its homepage) is used as a breach notice it will remain for 90 days or publish a conspicuous notice in print or broadcast media in geographic areas where individuals affected by the breach reside.

If more than 500 individuals in a single state or jurisdiction are affected, notice must be provided to prominent media outlets serving such state or jurisdiction (e.g., in the form of a press release). If there exists the possibility of imminent misuse of the unsecured PHI, telephone calls to affected individuals may also be appropriate.

Notifications must be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The notice must include certain specific information.

If the breach involves 500 or more individuals, DHHS must be notified immediately, which will subsequently post the breach on its website. If the breach involves less than 500 individuals, the covered entity must maintain a log and submit the log to DHHS on an annual basis.

Sanctions for Failing to Comply

Failure to comply with HIPAA can result in civil and criminal penalties.

Cival Penalties: There is a tiered civil penalty structure for HIPAA violations. The Secretary of the Department of Health and Human Services (DHHS) has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The Secretary is prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended).

Criminal Penalties: Covered entities and specified individuals whom "knowingly" obtain or disclose PHI face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Workforce Disciplinary Actions: Our company will take the following actions when an employee fails to comply with our HIPAA policies and procedures.

- **First Offense:** Verbal and written warning with explanation of specific violation or violations.
- **Second Offense:** Second verbal and written warning and retraining of policies and procedures at employees expense.
- **Third Offense:** Termination of employment.

HIPAA Policy and Training Manual

Appendix

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW HEARING HEALTHCARE INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.
THE PRIVACY OF YOUR HEALTH INFORMATION IS IMPORTANT TO US.

Our Legal Duty
We are required by applicable federal and state law to maintain the privacy of your health information. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your health information. We must follow the privacy practices that are described in this notice while it is in effect. This notice is effective starting June 12, 2006 and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and make the updated version available upon request.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the information listed at the end of this notice.

Use And Disclosure Of Your Health Information
We use and disclose health information about you for treatment, payment and healthcare operations. For example:

Treatment: We may use or disclose your health information to a physician or other healthcare provider who is treating you, including hearing aid manufacturers and other providers of hearing healthcare devices, and/or related supplies.

Payment: We may use and disclose your health information to obtain payment for services we provide you with.

Healthcare Operations: We may use and disclose your health information in connection with our healthcare operations. Healthcare operations include quality assessment and improvement activities, reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, conducting training programs, accreditation, certification, licensing or credentialing activities.

Your Authorization: In addition to our use of your health information for treatment, payment or healthcare operations, you may give us written authorization to use your health information or disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this notice.

To Your Family and Friends: We must disclose your health information to you, as described in the "Patient Rights" section of this notice. We may disclose your health information to a family member, friend or other person to the extent necessary to help with your healthcare or payment for your healthcare, but only if you agree that we may do so.

Persons Involved In Care: We may use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, your personal representative or another person responsible for your care, of your location, your general condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your healthcare. We will also use our professional judgment and experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up hearing aids, batteries, impressions, audiograms, or similar forms of health information.

Marketing Health-Related Services: We will not use your health information for marketing communications without your written authorization.

Required by Law: We may use or disclose your health information when we are required to do so by law.

Fundraising: We may provide medical information to one of our affiliated fundraising foundations to contact you for fundraising purposes. We will limit our use and sharing to information that describes you in general (not personally), including terms and dates of your health care. In any fundraising materials, we will provide you with a description of how you may choose not to receive future fundraising communications.

Abuse or Neglect: We may disclose your health information to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, domestic violence, or other crimes. We may disclose your health information to the extent necessary to avoid a serious threat to your health or safety and/or the health or safety of others.

National Security: We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose to correctional institutions or law enforcement officials having lawful custody of protected health information of inmate or patient under certain circumstances.

Appointment Reminders: We may use or disclose your health information to provide you with appointment reminders (such as voicemail messages, postcards, newsletters, or letters), as well as information about treatment alternatives.

Patient Rights Access: You have the right to view or receive copies of your health information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you requested unless we cannot practicably do so. You must make a request in writing to obtain access to your health information. You may obtain a form to request access by using the contact information listed at the end of this notice. You may also request access by sending us a letter to the address at the end of this notice. If you request copies, we may charge you $14 for 1-10 pages and $0.50 per page for pages 11-40, and $0.33 per page for every additional page. Actual postage costs will be added if you would like the information mailed to you. If you request an alternative format, we will charge a cost-based fee for providing your health information in that format. If you prefer, we will prepare a summary or an explanation of your health information for a fee. Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates have disclosed your health information for purposes, other than treatment, payment, healthcare operations and other activities, for the last 6 years, but not before June 12, 2006. If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restrictions: You have the right to request that we place additional restrictions on our use or disclosure of your health information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency).

Alternative Communication: You have the right to request that we communicate with you about your health information by alternative means or to alternative locations. You must make your request in writing. Your request must specify the alternative means or location, and provide satisfactory explanation about how payments will be handled under the alternative means and/or location you request.

Amendment: You have the right to request that we amend your health information. Your request must be in writing and explain why the information should be amended. We may deny your request under certain circumstances.

Electronic notice: If you receive this notice on our website or by electronic mail (e-mail), you are entitled to receive this notice in written form.

QUESTIONS AND COMPLAINTS

If you want more information about our privacy practices or have questions or concerns, please contact us.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may make us aware of your concern by using the contact information listed at the end of this notice. You may also submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to the privacy of your health information. We will not retaliate in any way if you choose to file a complaint with us or the U.S. Department of Health and Human Services.

Compliance Officer: Steve W. Barlow

Telephone: 1-888-906-7141

Address: 2501 Cottontail Lane, Ste. 101
Somerset, NJ 08873

Acknowledgment of Receipt of Privacy Practices Notice

By signing this form, you acknowledge receipt of our company's Notice of Privacy Practices. The Notice of Privacy Practices provides information about how we may use and disclose your protected health information. We encourage you to review it carefully. The Notice of Privacy Practices is subject to change. If the Notice is changed, you may obtain a revised copy by contacting us at the address below.

I acknowledge receipt of your Notice of Privacy Practices.

_____ _____

Patient Signature *Date*

Office Use Only

We attempted to obtain the patient's signature to acknowledge receipt of our *Privacy Practices Notice*, but were unable to do so. HIPAA laws require we keep record of attempt to obtain acknowledgment.

Date_____ Initials _____ Reason: _____

_____

RECORD OF ACKNOWLEDGMENT TO REMAIN IN PATIENT FILES AT ALL TIMES

Consent to Telephone Contact

I hereby give my consent for your company or entities calling on its behalf, to call my home or other alternative locations and leave a message on voice mail or in person in reference to carrying out treatment, payment or operational activities such as appointment reminders, insurance items and any calls pertaining to my hearing health care.

This permission shall remain in effect as long as I have not revoked my consent in writing and asked to be placed on your company's do-not-call list. Signing this form does NOT obligate me to make any purchases or otherwise respond to calls from the above listed company.

_____ _____

Patient Signature *Date*

Please fill in the phone number(s) we have your permission to use to contact you.

Home Phone _____ **Cell Phone** _____

2501 Cottontail Lane, Suite 101 • Somerset, NJ 08873

1-888-906-7141

Authorization to Release Health Information

Patient Name _____ _____ _____ Date Of Birth _____ / _____ / _____
First *Middle* *Last* *Month* *Date* *Year*

Address _____ Phone _____

_____

The patient listed above authorizes and requests the individual, organization or provider listed below:

Name _____

Address _____

_____

_____

To release the patient's healthcare information to:

Name _____

Address _____

_____

_____

Request and authorizations applies to:

Information

☐ All Medical Records, including but not limited to progress notes, operative notes, laboratory test results, diagnostic tests, and x-rays.

☐ Other _____

Dates of treatment

☐ All Dates

☐ Specific Dates _____

I hereby authorize the release of my medical records as described above. I understand that I may revoke this authorization at any time by notifying in writing the above named party.

_____ _____
Signature of Patient or Legal Representative Date:

This authorization will expire 90 days from the date signed.

2501 Cottontail Lane, Suite 101 • Somerset, NJ 08873
1-888-906-7141

Form #0015Gen;03 2015

Request for Restriction of Use and Disclosure Of Protected Health Information

Identification of patient requesting a restriction. *(Information below is needed for verification. Please print.)*

Patient Name _____ Date of Birth _____

Address _____ Date of Request _____

City, State, Zip_____

I hereby request the following restrictions be placed on uses and disclosure of my protected health information. I understand that your company is not required to agree to these restrictions if I do not provide appropriate billing information and an alternative address or method of contact, and that I will receive timely notification of this decision to comply or not to comply. I further understand that if the company agrees to comply with my request, they shall abide by the terms of my requested restrictions.

Types of protected health information to be restricted: _____

_____

_____

Requested restrictions on communications: _____

_____

_____

Requested address or method of contact: _____

_____

_____

_____ _____

Patient Signature *Date*

Submit requests to: Privacy Officer
2501 Cottontail Lane, Suite 101
Somerset, NJ 08873

For Office Use Only

Request Status
☐ Approved ☐ Denied
Date of decision _____

Privacy Officer_____

Signature _____

HIPAA Privacy Violation Complaint Form

Person Filing Complaint:

Today's Date _____ / _____ / _____
Month *Date* *Year*

Name_____ _____
First *Last*

Phone _____

Address _____

Email _____

_____

Incident Details

This report is filed for: ☐ The person listed above. ☐ On behalf of _____ _____
First Name *Last Name*

Date of incident _____ / _____ / _____
Month *Date* *Year*

Time of incident (approximately) _____

Office location of incident: City _____ State_____

Please briefly describe what happened and why you believe your (or someone else's) HIPAA privacy rights were violated.

_____

_____

_____

_____

_____

_____

_____

_____

Signature of person filing complaint _____

Notice of Confidentiality

Information pertaining to investigation of this complaint will only be shared with those who have a need to know. Confidentiality of all participants in the reported situation shall be maintained to the extent reasonably possible throughout any resulting investigation. The investigator(s) will conduct the necessary and appropriate investigation commensurate with the level of complaint and the specific facts. This investigation may include, but is not limited to, interviewing the individuals involved, interviewing other individuals, obtaining specific facts surrounding the violation/breach and reviewing pertinent documentation.

Please mail completed form to the address below, to the attention of the Compliance Officer.

2501 Cottontail Lane, Suite 101 • Somerset, NJ 08873
1-888-906-7141

Form #0024Gen; 03 2015

Business Associate Agreement

Business Associate _____ Covered Entity _____

Address _____ Date of Agreement _____

_____

The Business Associate and the Covered Entity listed above have entered into the Business Associate Agreement ("BAA" or "Agreement") described below.

WITNESSETH:

The Business Associate listed above and "_____" (the Covered Entity) have entered into the Business Associate Agreement ("BAA" or "Agreement") described below.

WITNESSETH:

WHEREAS, "_____" and Business Associate are Parties to an Agreement, of which this Business Associate Agreement is incorporated, that contains express and implied mutual promises and covenants that in some instances require the use or disclosure of Protected Health Information ("PHI");

WHEREAS, the Health Insurance Portability and Accountability Act's ("HIPAA") Privacy Regulations as amended by Health Information Technology for Economic and Clinical Health ("HITECH") provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA"), require a Covered Entity to enter into a Business Associate contract with "_____", so that "_____". may obtain PHI from or on behalf of a Covered Entity;

WHEREAS, a condition in the Business Associate contract is that "_____" must ensure that every contractor or agent, to whom "_____" provides PHI received from a Covered Entity or obtains on behalf of a Covered Entity, agrees to the same restrictions and conditions that apply to "_____" through the Business Associate contract;

WHEREAS, "_____" understands that it must enter into this Agreement so that PHI may be disclosed to Business Associate and to allow Business Associate to perform and provide services to "_____" as part of the Subcontract Agreement.

NOW, THEREFORE, in consideration of the Parties' continuing obligation as set forth in the Agreement and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement to comply with the Privacy and Security Regulations and to protect the interests of both Parties:

I. Background and Purpose

(a) Covered Entity is subject to and must comply with the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the

Form #0026AV-1; 03 2015

HITECH provisions of ARRA and all regulations promulgated pursuant to authority granted therein;

(b) Business Associate constitutes a Business Associate of Covered Entity (as such term is defined in the Regulations, see 45 CFR 160.103) and wishes to commence or continue its business relationship with Covered Entity;

(c) Business Associate acknowledges that Covered Entity must comply with the regulations at CFR at Title 45, Sections 160 and 164 and that to achieve such compliance, the written agreement between Covered Entity and Business Associate must contain certain satisfactory assurances that Business Associate will appropriately safeguard Protected Health Information (as that term is defined in Federal regulations at 45 CFR 164.501) which it receives from, or creates or receives on behalf of Covered Entity.

(d) Business Associate acknowledges that Business Associate must comply with all provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") pursuant to the terms of the HITECH provisions of ARRA.

II. Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Privacy and Security Rule ("the Rule") as amended by HITECH provisions of ARRA,, which is defined for purposes of this Agreement as the Code of Federal Regulations ("C.F.R.") at Title 45, Parts 160 and 164 as amended from time to time.

(a) **Business Associate.** "Business Associate" shall mean the party identified as the Business Associate in the first Paragraph of this Business Associate Agreement.

(b) **Covered Entity.** "Covered Entity" shall mean **"**_____**"**.

(c) **Designated Record Set.** "Designated Record Set" has the same meaning as this term has in 45 CFR §164.501.

(d) **Discovery.** "Discovery" shall mean the first day on which a breach is known to the Business Associate (including any person, other than the individual committing the breach that is an employee, officer, or other agent of Business Associate), or should reasonably have been known to Business Associate, to have occurred.

(e) **Electronic Health Record.** "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

(f) **Individual.** "Individual" has the same meaning as this term has in 45 CFR §164.501.

(g) **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E., as amended by the HITECH provisions of ARRA.

(h) **Protected Health Information.** "Protected Health Information" (or "PHI") has the same meaning as this term has in 45 CFR §160.103 (as amended by the HITECH provisions of ARRA), limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(i) **Required By Law.** "Required By Law" has the same meaning as this term has in 45 CFR §164.501.

(j) **Secretary.** Shall mean the Secretary of the Department of Health and Human Services or his or her designee.

(k) **Security Breach.** "Security Breach" has the same meaning as this term has in §13400 of HITECH provisions of ARRA, or means the unauthorized acquisition, access, use or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Security Breach does not include:

a. Any unintentional acquisition, access, or use of Protected Health Information by an employee or individual under the authority of the Business Associate if:

   i. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with Business Associate; and

   ii. Such information is not further acquired, accessed, used or disclosed by any person; or

b. Any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by Business Associate to another similarly situated individual at the same facility; and

c. Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization b any person.

(l) **Security Breach Compliance Date.** "Security Breach Compliance Date" means the date that is thirty (30) days after the Secretary publishes interim final regulations to carry out the provisions of Section 13402 of Subtitle D (Privacy) of ARRA which date is September 24, 2009.

(m) **Unsecured Protected Health Information.** "Unsecured Protected Health Information" means protected health information, in any form or medium, including electronic, paper, or oral form, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or

methodology, such as encryption and destruction of the information, as specified by the Secretary in guidance as issued by the Secretary from time to time. Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

a. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

    i. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

    ii. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs,* or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

b. The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

    i. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

    ii. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

III. Obligations and Activities of Business Associate

(a) Business Associate agrees not to use or disclose Protected Health Information other than as permitted by this BAA or as required by law. Business Associate acknowledges that, effective the later of the Effective Date of this Agreement or February 17, 2010, it shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with any of the use and disclosure requirements of this Agreement and any guidance issued by the Secretary from time to time with respect to such use and disclosure requirements.

(b) Business Associate agrees that beginning on the effective date of this Agreement or the Security Breach Compliance Date it will report to Covered Entity any Security Breach of Unsecured Protected Health Information without unreasonable delay and in no case later than the time period allowed in any applicable underlying contract or later than sixty (60) calendar days after Discovery of a Security Breach, as applicable. Such notice shall include the identification of each individual whose Unsecured Protected Health Information has been or is reasonably believed by Business Associate, to have been, accessed, acquired, or disclosed during such Security Breach. In addition, Business Associates shall provide any additional information reasonably requested by Covered Entity for purposes of investigating the Security Breach, Business Associate's notification of a Security Breach under this section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

(c) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this BAA or as required by law, and to implement administrative, physical, and technical safeguards that are reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits and as are otherwise required by ARRA and related guidance issued by the Secretary from time to time.

(d) Business Associate agrees to mitigate, to the extent practicable, any harmful effect of any use or disclosure that is known to Business Associate to have occurred in violation of the terms of this BAA.

(e) All reporting required of Business Associate under the terms of this Business Associate Agreement shall be made in writing addressed to

Attn: Steve W. Barlow
Privacy and Compliance Officer
2501 Cottontail Lane, Suite 101
Somerset, NJ 08873
Phone: 1-888-906-7141

(f) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information, and agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits. With respect to Electronic Protected Health Information, Business Associate shall implement and comply with (and ensure that its subcontractors implement and comply with) the administrative safeguards set forth at 45 C.F.R. 164.308, the physical safeguards set forth at 45 C.F.R. 310, the technical safeguards set forth at 45 C.F.R. 164.312, and the policies and procedures set forth at

45 C.F.R. 164.316 to reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate acknowledges that, effective the later of the Effective Date of this Agreement or February 17, 2010,

a. The foregoing safeguard, policies and procedures requirements shall apply to Business Associate in the same manner that such requirements apply to Covered Entity, and

b. Business Associate shall be liable under the civil and criminal enforcement provisions set forth in 42 U.S.C. 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with the safeguard, policies and procedures requirements and any guidance issued by the Secretary from time to time with respect to such requirements.

(g) Business Associate agrees to report any security incidents, as defined by the Rule and HITECH provisions of ARRA, to the Covered Entity.

(h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to Covered Entity and/or to the Secretary of the United States Department of Health and Human Services, within ten (10) business days of receiving such request, or at such other time as may be designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Rule and the HITECH provisions of ARRA and related guidance as issued by the Secretary from time to time.

(i) Business Associate agrees to document such disclosures of Protected Health Information (PHI) and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual or an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528 and the HITECH provisions of ARRA and related guidance as issued by the Secretary from time to time.

(j) Business Associate agrees to provide to Covered Entity or the Individual to whom PHI relates, upon request and within ten (10) business days of receiving such request, information collected in accordance with Section III (g) of this BAA and sufficient to constitute, or permit Covered Entity to provide, a response to a request by the Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. In addition, with respect to information contained in an Electronic Health Record, Business Associate shall document, and maintain such documentation for three years from date of disclosure, such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of information contained in an Electronic Health Record, as required by Section 13405(c) of Subtitle D (Privacy) of ARRA and related regulations issued by the Secretary from time to time.

(k) Business Associate agrees to provide access, at the request of Covered Entity, within ten (10) business days to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an individual in order to meet the requirements under 45 C.F.R. 164.524 and Section 13405(e) of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

(l) Business Associate agrees to promptly make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of Covered Entity or an Individual to whom the PHI pertains.

IV. Permitted Uses and Disclosures by Business Associate

(a) Business Associate shall be permitted to use and/or disclose Protected Health Information provided or made available from Covered Entity to complete any and all services agreed to under the Agreement, Subcontract or other Service Agreement between the parties and any corresponding Statement(s) of Work, provided that such use or disclosure would not violate the Privacy Rule or ARRA if done by the Covered Entity.

(b) Except as otherwise limited in this BAA, Business Associate acknowledges that it shall request from Covered Entity and so disclose to its affiliates, agents and subcontractors or other third parties, only

a. The information contained in a "limited data set," as such term is defined at 45 C.F.R. 164.514(e) (2), or,

b. If needed by Business Associate, to the minimum necessary to accomplish the intended purpose of such requests or disclosures. In all cases, Business Associate shall request and disclose Protected Health Information only in a manner that is consistent with guidance issued by the Secretary from time to time.

(c) Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the Rule or ARRA (including the minimum necessary standard established by the Rule or ARRA) if done by the Covered Entity or violate the policies and procedures of the Covered Entity.

(d) Except as otherwise limited in this BAA, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate, provided that the disclosures are required by law within the meaning of the Rule or ARRA or any guidance as issued by the Secretary from time to time or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law

or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

(e) Except as otherwise limited in this BAA, Business Associate may use Protected Health Information to provide Data Aggregation services relating to the health care operations of the Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

(f) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1)

V. Obligations of Covered Entity

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

(d) Permissible requests by Covered Entity: Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except that this restriction is not intended, and shall not be construed, to limit Business Associate's capacity to use or disclose Protected Health Information for the proper management and administration of the Business Associate or to provide Data Aggregation services to Client, as provided for and expressly permitted under Section IV. (b), (c), and (d) of this BAA.

VI. Term and Termination

(a) **Term.** The Term of this BAA shall be effective upon execution, and shall terminate when the contractual or other relationship between Covered Entity and Business Associate that involves or requires the receipt, creation, use, and/or disclosure of PHI by or to the Business Associate is terminated or ceases to exist.

(b) **Termination for Cause.** Upon the Covered Entity obtaining knowledge of a pattern of activity or practice by Business Associate that constitutes a material breach or violation of Business Associate's obligations under this BAA, Covered Entity shall

a. Provide an opportunity for Business Associate to cure the breach or end the violation within ten (10) days of receiving notice of the breach and/or violation, and, if such action does not successfully bring about cure of the breach or an end to the violation within the time specified by Covered Entity; shall terminate this BAA and the underlying contract or relationship under which the Business Associate has access to, uses or discloses PHI on behalf of Covered Entity; or

b. Immediately terminate this BAA and the underlying contract or relationship under which the Business Associate has access to, uses or discloses PHI on behalf of Covered Entity, if cure of the breach or causing the violation to end is not possible; or

c. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) **Obligations of Business Associate Upon Termination**

Except as provided in paragraph b of this subsection, upon termination of this BAA, for any reason, Business Associate shall return to Covered Entity or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall also apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

In the event that return or destruction of any Protected Health Information is not feasible, Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information

(d) **State Law.**

If state law applicable to the relationship between Business Associate and Covered Entity contains additional or more stringent requirements than federal law for Business Associates regarding any aspect of PHI privacy or security, then Business Associate agrees to comply with the higher standard contained in applicable state law.

VII. Miscellaneous

(a) **Regulatory References.** A reference in this BAA to a section in the Privacy Rule means the section as in effect or as amended.

(b) **Amendment.** This BAA may only be modified through a writing signed by the Parties and, thus, no oral modification hereof shall be permitted. Covered Entity and Business Associate agree to take such action as is necessary to amend this BAA from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule, ARRA and HIPAA.

(c) **Survival.** The respective rights and obligations of Business Associate under Section VI (c) of this BAA shall survive the termination of this Agreement.

(d) **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

(e) **Notice to Covered Entity.** Any notice required under this BAA to be given Covered Entity shall be made in writing to:

Attn: Steve W. Barlow
Privacy and Compliance Officer
2501 Cottontail Lane, Suite 101
Somerset, NJ 08873

(f) **Notice to Business Associate.** Any notice required under this BAA to be given Business Associate shall be made in writing to:

_____

_____

_____

* * * * * *

IN WITNESS WHEREOF, Covered Entity and Business Associate have caused this Business Associate Agreement to be executed by duly authorized officers.

"_____"	BUSINESS ASSOCIATE
By: _____	By: _____
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____
Date: _____	Date: _____

Form #0026AV-10; 03 2015