**LARRY GRUDZIEN**

**ATTORNEY AT LAW**

**708 SOUTH KENILWORTH AVENUE**

**OAK PARK, ILLINOIS 60304-1132**

**(708) 717-9638**

**HIPAA PRIVACY FORMS COMPLIANCE PACKAGE FOR EMPLOYER GROUP HEALTH PLANS (‘COVERED ENTITIES”)**

Under the Privacy Rule, employer group health plans that are not in compliance can face civil and criminal penalties. These penalties are based on a tiered approach, as follows:

* No Knowledge. Where a person does not know, and by exercising due diligence would not have known, that the person violated HIPAA's administrative simplification provisions, the minimum penalty is $100 per violation. The maximum penalty is $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
* Reasonable Cause. Where a violation is due to “reasonable cause” and not “willful neglect,” the minimum penalty is $1,000 to $50,000 per violation. The maximum penalty is $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
* Willful Neglect (but Corrected). Where a violation is due to “willful neglect,” but was corrected, the minimum penalty is $10,000 to $50,000 per violation. The maximum penalty is capped at $1.5 million for violations of an identical requirement or prohibition within the same calendar year.
* Willful Neglect (but not Corrected). Where a violation is due to “willful neglect,” but was not corrected, the minimum penalty is $50,000 per violation; there is no maximum per violation. The total penalty is capped at $1.5 million for violations of an identical requirement or prohibition within the same calendar year.

The following is a complete package of all HIPAA Privacy Forms for employer group health plans (“Covered Entities”) and it is ready and waiting for your immediate use to help you meet the new requirements. This package has been drafted to comply with all of the new HIPAA regulations and you need only add a few pieces of information.

The HIPAA Privacy Forms Compliance Package for Employer Group Health Plans (“Covered Entities”) contains:

* An Explanation of HIPAA Privacy Rules,
* A Summary of New HIPAA Regulations,
* A HIPAA Privacy Policy,
* A HIPAA Use and Disclosure Form,
* A Notice of Privacy Practices,
* A Business Associates Agreement,
* An Authorization for Release of Information,
* A HIPAA Security Standards Checklist,
* A Plan Sponsor Certification Form,
* A HIPAA Privacy Compliance Checklist,
* A Plan Amendment for Privacy Practices,
* A Summary of Material Modifications to amend the Employer's SPD,
* A HIPAA Training Acknowledgment,
* A Request for Alternative Communications,
* A Request for an Accounting or Disclosure of Protected Health Information,
* A Request to Amend or Correct Protected Health Information, and
* A Request to Inspect or Copy Protected Health Information.

If you have any questions, please call me at above number or email me at:

larry@larrygrudzien.com

**EXPLANATION OF HIPAA PRIVACY RULES**

**Q/A-1 What are the administrative simplification requirements created under the Health Insurance Portability and Accountability Act (HIPAA)?**

HIPAA’s administrative simplification requirements were designed in part to reduce health care costs by standardizing the electronic processing of health care claims. The three primary components are:

* Privacy standards*,* addressing who is authorized to access information and the right of individuals to determine how their information is to be used or disclosed.
* Security standards, addressing the ability to control access and to protect information from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration, destruction, or loss.
* Transaction standards*,* promoting the standardization of certain payment-related electronic transactions (also referred to as the electronic data interchange or “EDI” standards).

**Q/A-2 What entities must comply with the administrative simplification requirements?**

These standards apply to all “covered entities”, including:

* Health plans;
* Health care clearinghouses (certain entities that process or facilitate the processing of health information);
* Health care providers that conduct certain types of transactions in electronic form;
* Enrolled sponsors of the Medicare prescription drug discount card; and
* Business associates, such as TPAs, attorneys, accountants, consultants, health information organizations, e-prescribing gateways, data transmission entities, entities that maintain PHI for a covered entity, and subcontractors of a covered entity.

A group health plan that will disclose Protected Health Information (PHI) to the plan sponsor must obtain a certification from the sponsor that certain provisions have been added to the plan document and the Summary Plan Description and that the sponsor will abide by those provisions.

See the PLAN SPONSOR CERTIFICATION FORM, the PLAN AMENDMENT FOR PRIVACY PRACTICES and the SUMMARY OF MATERIAL MODIFICATIONS to amend the Employer's SPD.

**Q/A-4 Are there special requirements for business associates involved in the use or disclosure of PHI?**

The American Recovery and Reinvestment Act of 2009 (ARRA) made changes to HIPAA and requires that all business associates comply with the security and privacy requirements of HIPAA. Covered entities often use business associates such as TPAs, attorneys, accountants, and consultants to assist them in performing plan functions. When such functions involve the use or disclosure of PHI, the covered entity and the business associate must enter into a “business associate contract” imposing specific obligations on the business associate.

Business associates are required to:

* Comply directly with the security rule provisions directing implementation of administrative, physical and technical safeguards for electronic PHI and development and enforcement of related policies, procedures, and documentation standards (including designation of a security official);
* Impose an obligation to directly comply with HIPAA’s business associate safeguards, including limiting use and disclosure of PHI as specified in the agreement or as required by law; facilitating access, amendment and accounting of disclosures; opening books and records to the Department of Health and Human Services (HHS); and returning or destroying PHI, if feasible, upon contract termination;
* Comply with the notification requirements upon a breach, which is defined as the “unauthorized acquisition, access, use, or disclosure of PHI;
* Comply with restrictions on disclosures to health plans, minimum necessary standards, accounting requirements applicable to electronic health records and prohibitions on sales of PHI; and
* Require that their subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate comply with HIPAA Rules.

A business associate will be deemed to violate HIPAA if it knows of a “pattern of activity or practice” by a covered entity that breaches their business associate agreement, but fails to cure the breach, terminate the business associate agreement, or report the non-compliance to HHS. Additionally, civil and criminal penalties, notification provisions for a breach, and application of guidance on the most effective and appropriate technical safeguards as determined by the HHS are also applicable to business associates.

A covered entity that knows of a business associate’s material violation of the business associate contract must take reasonable steps to cure the breach or end the violation. If those steps are unsuccessful, then the covered entity must terminate the business associate contract or, if that is not feasible, report the business associate to HHS. In other words, covered entities cannot avoid responsibility by intentionally ignoring problems.

**Q/A-5 What information is covered under the privacy requirements?**

The privacy requirements generally cover “individually identifiable health information” transmitted or maintained in any form or medium (electronic or otherwise), while the security requirements apply to “electronic PHI” (defined below). When such information is created or received by a covered entity (or by a plan sponsor or business associate acting on behalf of the covered entity), it becomes “protected health information” (PHI) subject to the privacy rule. HIPAA provides specific detailed definitions for these terms, which are summarized below:

* “Health information*”* is the broadest term. It refers to information, whether oral or communicated in any medium, that relates to an individual’s medical condition, the provision of medical care for that individual, or the payment for that individual’s medical care. This term is broad enough to pick up health coverage enrollment and premium payment information as well as information relating to health condition and treatment.
* “Individually identifiable health information*”* is health information that identifies the individual to whom it relates and is created or received by a covered entity or an employer.
* “Protected health information”is individually identifiable health information that is maintained or transmitted by a covered entity, subject to certain exceptions.
* “Electronic protected health information*”* is protected health information that is transmitted by or maintained in electronic media. (Note that all electronic PHI is PHI and is therefore subject to the privacy rule as well as subject to the security rule.)

**Q/A-6 How do the privacy and security rules affect group health plans and plan sponsors?**

HIPAA’s privacy standards impose rules for use and disclosure of PHI. Under the privacy standards, individuals are entitled to certain rights with respect to their health information, and covered entities must provide privacy notices and comply with certain administrative requirements to protect the privacy of PHI. Covered entities must establish policies reflecting the privacy and security requirements.

HIPAA’s security standards impose rules for the protection of electronic PHI. Covered entities must, among other things, perform a risk analysis and implement a risk management plan to protect the confidentiality, integrity, and availability of electronic PHI.

For purposes of the privacy and security rules, employers (as plan sponsors) and TPAs normally will not be covered entities. However, the privacy and security rules generally will apply to group health plans and therefore plan sponsors will be affected. Moreover, plan sponsors must agree to protect PHI that they receive from their health plans and insurers. Health plans and other covered entities must obtain the agreement of their TPAs and other business associates to protect the privacy of PHI and the security of electronic PHI.

See BUSINESS ASSOCIATES AGREEMENT contained in this package.

Thus, although they do not directly cover plan sponsors, the privacy and security rules will have a significant impact upon the health plan of plan sponsors.

The size of the compliance burden imposed on group health plans and their plan sponsors by the HIPAA privacy and security rules will depend on the plan sponsor’s role in the plan’s administration and whether the plan has its own employees, premises, hardware, or software. In addition, for privacy purposes, whether the plan is insured is a relevant factor. As explained below, a group health plan and its plan sponsor may avoid many of HIPAA’s privacy requirements if the plan is fully insured and if the plan sponsor has no access to PHI other than summary health information and enrollment information. A self-funded group health plan and its plan sponsor will have more obligations under the privacy standards. The security rule focuses on the protection of electronic PHI and in large part addresses the covered entity’s employees, premises, hardware, software, and electronic media. For purposes of security compliance, plans that have their own employees, premises, hardware, software, or media will have a heavier compliance burden than will plans that use the services of business associates and the plan sponsor to handle electronic PHI.

See the HIPAA PRIVACY POLICY AND PROCEDURES and the HIPAA PRIVACY COMPLIANCE CHECKLIST contained in this package

**Q/A-7 What are the rules regarding sharing group health plan PHI with the plan sponsor?**

The privacy and security standards address a group health plan’s ability to share PHI and electronic PHI with a plan sponsor. The rules generally prohibit a group health plan from sharing PHI or electronic PHI with a plan sponsor except in the following circumstances:

* A group health plan (or its health insurance issuer or HMO) may disclose “summary health information” to the plan sponsor, upon request, for the limited purposes of obtaining premium bids for providing health insurance coverage under the group health plan or modifying, amending or terminating the group health plan.

“Summary health information” is information that summarizes the claims history, expenses, or types of claims by individuals for whom the plan sponsor has provided health benefits under a group health plan. Names and certain other identifying information must be removed.

* A group health plan (or its health insurance issuer or HMO) may disclose information regarding whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, to a plan sponsor without complying with the plan document and firewall requirements otherwise required when a group health plan shares PHI with a plan sponsor.
* A group health plan (and its insurer or HMO) may disclose PHI to plan sponsors for “plan administration functions” such as quality assurance, claims processing, auditing, and monitoring in connection with the health plan, if the plan sponsor agrees in the plan document to limitations on the use and disclosure of the PHI. The plan must be amended to establish the permitted and required uses and disclosures of PHI by the plan sponsor. In addition, the plan document must specify that disclosure is permitted only upon receipt of written certification that the plan documents have been amended to include certain specific restrictions and that the plan sponsor agrees to those restrictions. Finally, the plan document must require the employer to maintain adequate “firewalls,” which means that the plan document must:
  + Describe the employees (or class of employees) or other persons under the control of the plan sponsor who may be given access to PHI;
  + Restrict access to and use by such individuals to plan administration functions that the plan sponsor performs for the health plan; and
  + Provide a procedure for resolving any issues of noncompliance by such individuals.

If the PHI that will be disclosed to plan sponsors for plan administration functions is electronic PHI, more is required. Electronic PHI is of course PHI, so the privacy provisions outlined above must be in place. In addition, the plan document must be amended to require the plan sponsor to:

* + Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the plan sponsor creates, receives, maintains, or transmits on behalf of the plan;
  + Ensure that the firewall required by the privacy amendment is supported by reasonable and appropriate security measures;
  + Ensure that any agent or subcontractor to whom the plan sponsor provides the electronic PHI agrees to implement reasonable and appropriate security measures to protect the electronic PHI; and
  + Report to the plan any security incident of which the sponsor becomes aware.
* Covered entities may use and disclose PHI with an individual’s authorization for essentially any purpose specified in the authorization. A group health plan may not condition treatment or payment on an authorization, except that, in general, a health plan may condition enrollment on provision of an authorization, so long as the authorization is requested prior to the individual’s enrollment and is sought for the plan’s eligibility and enrollment determinations, or for its underwriting or risk determinations.

Unless an authorization is received from the individual, group health plans are specifically prohibited from disclosing information to a plan sponsor for employment-related actions or decisions or in connection with any other benefit. And the notice of privacy practices must explain the types of disclosures that may be made by the health plan under these rules, unless the only disclosures are pursuant to an authorization.

See the AUTHORIZATION FOR RELEASE OF INFORMATION contained in this package.

**Q/A-8 What are the use and disclosure rules for PHI?**

Covered entities are prohibited from disclosing or using PHI except as permitted under the privacy standards. Under the use and disclosure rules, covered entities may use and disclose PHI for treatment, payment, and health care operations. Further disclosure generally requires an authorization, unless an exception applies.

Minimum-Necessary Standard

Many disclosures are subject to a “minimum-necessary” standard. Under this standard, a covered entity must reasonably ensure that any PHI used, disclosed, or requested is limited to the minimum information necessary to accomplish the intended purpose of the use, disclosure, or request.

* For its own uses of information, a covered entity must identify (by name or classification) who within its workforce needs access to PHI to carry out their duties and must take steps to ensure that only those persons have such access.
* For disclosures and requests for disclosure of PHI that are routine and recurring, a covered entity must develop policies and procedures that limit the amount disclosed or requested to the minimum amount necessary.
* For all other disclosures and requests, a covered entity must develop criteria designed to limit the amount of information disclosed or requested, and it must review all requests for disclosure on an individual basis in accordance with those criteria. The minimum-necessary standard does not apply to disclosures made by a covered entity pursuant to an individual authorization.

Required Disclosures

The privacy standards require disclosure of PHI in only two circumstances:

* Disclosures are required to be made to individuals who exercise their individual rights; and
* Disclosures must be made to HHS in connection with its enforcement and compliance review actions.

Use or Disclosure Pursuant to Authorization

An individual’s authorization allows a covered entity to use and disclose the PHI described in the authorization for essentially any purpose specified in the authorization.

**Q/A-9 Are there any exceptions to the use and disclosure rules of PHI?**

Covered entities may disclose PHI without authorization for specified “public policy” purposes, such as judicial and administrative proceedings or to avert a serious threat to health or safety. These public policy exceptions are available only when specific conditions are satisfied. And even when disclosure is permitted, the PHI that may be disclosed is limited to the minimum necessary for the particular purpose. In certain limited situations, a covered entity may use or disclose certain PHI without an authorization, if the individual has been given the opportunity to agree or object to the disclosure of such information in accordance with specific procedures. This rule permits disclosures of limited types of information to family members, close personal friends of the individual, and others identified by the individual for certain purposes such as involvement in care or payment and disaster relief.

The privacy standards allow covered entities to freely use and disclose “de-identified” information. For information to be considered de-identified, the covered entity must either obtain a professional statistical analysis that the information is not individually identifiable or delete 18 specific identifiers (e.g., name, Social Security number, address, ZIP code). The covered entity may not disclose the key or other mechanism by which the information could be re-identified, except under circumstances that would permit disclosure of the underlying information.

**Q/A-10 What rights does an individual have with respect to their health information?**

Under the privacy standards, individuals are granted certain rights with respect to their health information, including the right to:

* Inspect and obtain a copy of their own PHI;
* Amend or correct PHI that is inaccurate or incomplete;
* Obtain an accounting of certain disclosures of their PHI that were made by covered entities (with some exceptions, which include disclosures made for purposes of treatment, payment, or health care operations and disclosures made to the individual or pursuant to the individual’s authorization);
* Receive the notice of privacy practices required under the privacy standards (described below);
* Receive notice of any breach of the individual’s PHI; and
* Request additional restrictions on the use or disclosure of their own PHI (although the covered entity may deny this type of request).

The privacy standards require a covered entity to respond within a specified time to an individual’s request to inspect, copy, or amend PHI or for an accounting.

See the REQUEST FOR ALTERNATIVE COMMUNICATIONS, the REQUEST FOR AN ACCOUNTING OR DISCLOSURE OF PROTECTED HEALTH INFORMATION, the REQUEST TO AMEND OR CORRECT PROTECTED HEALTH INFORMATION, and the REQUEST TO INSPECT OR COPY PROTECTED HEALTH INFORMATION contained in this package.

**Q/A-11 What notices are required to be provided to individuals regarding privacy practices for PHI?**

Covered entities are required to provide individuals with a notice of their privacy practices for PHI. This notice must describe:

* The uses and disclosures of PHI that may be made by the covered entity;
* The individual’s rights; and
* The covered entity’s legal duties with respect to the PHI.

Privacy notices must satisfy specific content requirements, must be written in plain language, and must reflect the covered entity’s actual practices, not simply reiterate the regulations. Privacy notices must be provided to those individuals whose PHI will be used or maintained by the covered entity. A single notice to the named insured or covered employee is effective for all covered dependents under a health plan. Notices must be provided:

* At the time of an individual’s enrollment in the plan or, in the case of providers, at the time of treatment and consent; and
* Within 60 days after a material change to the notice.

In addition, plans must notify participants at least once every three years that a notice of privacy practices is available.

A fully insured plan’s obligation to provide a privacy notice depends on whether the plan has access to PHI (except for summary health information and enrollment information). If the plan has no access to PHI (except for summary health information and enrollment information), it has no obligation to provide a notice—the notice requirement is imposed solely upon the insurer. However, if a fully insured plan has access to PHI (other than summary health information and enrollment information), then the plan must maintain a notice and provide it upon request. (The insurer still has the primary notice obligation.) Self-funded group health plans must issue their own privacy notices.

See the NOTICE OF PRIVACY PRACTICES contained in this package.

**Q/A-12 What are the administrative requirements for protecting the privacy of PHI?**

The privacy standards also require covered entities to take the following actions to protect the privacy of PHI:

* Designate a privacy official responsible for the development and implementation of privacy policies and procedures and a contact person (the privacy official or another person) or office for receiving complaints and providing additional information concerning the privacy notice;
* Train their workforces on privacy policies and procedures;
* Establish appropriate safeguards for protecting the privacy of PHI from accidental or intentional use or disclosure in violation of the privacy standards (such as limiting access to information by creating computer firewalls and locking doors or filing cabinets);
* Create a process for individuals to lodge complaints and a system for handling such complaints, and keep a record of the complaints and any resolution;
* Design a system of written disciplinary policies and sanctions for workforce members who violate the covered entity’s privacy policies and procedures;
* Mitigate, to the extent practicable, any harmful effect that is known to the covered entity resulting from an improper use or disclosure of PHI;
* Notify applicable individuals/entities/agencies of any breaches of PHI;
* Refrain from intimidating or retaliating against individuals or others for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the privacy standards;
* Not require individuals to waive their rights under the privacy standards; and
* Implement policies and procedures designed to comply with the privacy standards.

Covered entities are required to document their policies and procedures and maintain the documentation for at least six years.

These administrative requirements (other than the prohibitions on intimidating or other retaliatory actions and requiring individuals to waive their privacy rights) do not apply to a fully insured group health plan with no access to PHI except summary and enrollment information. The requirements would, however, apply to the health insurer.

See the HIPAA TRAINING ACKNOWLEDGMENT contained in this package.

**Q/A-13 What are the requirements for covered entities that electronically maintain or transmit PHI?**

HIPAA requires health plans and other covered entities that electronically maintain or transmit PHI to implement reasonable and appropriate safeguards to:

* Ensure the availability, integrity, and confidentiality of electronic PHI;
* Protect against reasonably anticipated threats to security and reasonably anticipated uses or disclosures of information that are not permitted by the privacy rule; and
* Otherwise ensure compliance with the security standards by their workforce.

HHS has issued its final security rule addressing security standards and safeguards for electronic PHI.

The security rule—

* Applies the new security standards to all electronic PHI that is maintained or transmitted by a covered entity;
* Sets forth specific security standards that covered entities are required to follow. These security standards are divided into three groups (administrative safeguards, physical safeguards, and technical safeguards) that must be put into place in order to guard data integrity, confidentiality, and availability; and
* Sets forth implementation specifications for each security standard. The implementation specifications are divided into two groups: required and addressable. Addressable does not mean optional, and the security rule sets out a series of steps that a covered entity must perform, and document in determining whether the implementation specification, an equivalent alternative, or nothing is needed to protect the electronic PHI. Thus, covered entities have some flexibility in determining specific procedures for complying with each security standard.

Although the security rule applies only to electronic PHI, there is significant overlap between the security rule’s safeguard requirements and the privacy rule’s safeguard requirements. Covered entities will need to analyze their own situation to determine the extent to which security standards should be implemented immediately (before the security rule’s compliance date), and with respect to all PHI (not just electronic PHI as required by the security rule).

The security rule also requires that a plan amendment be in place if the plan sponsor will create, receive, maintain, or transmit electronic PHI on behalf of the plan, and that a business associate contract be in place if the plan will disclose electronic PHI to third parties that are acting on behalf of the plan.

See the HIPAA SECURITY STANDARDS CHECKLIST in this package.

**Q/A-14 What are the electronic data standard requirements under HIPAA?**

HIPAA’s EDI Standards require health plans and other covered entities (and their business associates) that engage in certain “covered transactions” to use standardized formats and content, as well as uniform codes to conduct such transactions. Regulations set forth a specific standard format and content requirements that have been adopted for each of these transactions. Generally, these standards have been developed by the industry and are already in use, although not consistently. Covered entities also must identify medical conditions and procedures using uniform code sets.

Generally, if a covered entity or its business associate conducts a covered transaction electronically with another such entity, the transaction will be subject to the EDI Standards. Covered transactions include health claims, benefit payments, coordination of benefits, enrollment in a health plan, and certain other transactions.

In many cases, electronic transactions will not need to comply because the party sending or receiving the transmission is not a covered entity. For example, health plans may continue to accept data in a non-standard format from a non-covered entity (e.g., eligibility information from a plan sponsor). However, the EDI Standards apply to internal transactions within a covered entity that fit the definition of a covered transaction.

The EDI Standards include additional requirements for health plans. A health plan must, among other things:

* Conduct a transaction as a standard transaction if another entity so requests;
* Not delay, reject, or otherwise adversely affect a transaction because it is a standard transaction;
* Not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan; and
* Not require providers to make changes or additions to the standard transaction.

An entity that is not a covered entity under HIPAA, including an employer acting in the role of a plan sponsor, is not required to comply with the EDI Standards. However, non-covered entities are encouraged to use standard transactions.

HIPAA’s EDI Standards do not apply to transactions conducted solely by paper or by telephone. The EDI Standards allow covered entities to use a clearinghouse to convert data between nonstandard and standard formats, and they also contain certain other exceptions.

**Q/A-15 What are a covered entity’s responsibilities if a breach of PHI occurs?**

Covered entities have certain notification requirements in the event of a breach of “unsecured protected health information.” A breach is defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the privacy rule which compromises the security or privacy of such information. Unsecured protected health information is defined as protected health information that the covered entity or business associate has not secured via standards approved by the Secretary.

Generally, the notification of a breach must be provided “without unreasonable delay”, but in no case later than 60 days after dater in which the breach was discovered. For this purpose, discovery means the first day on which an employee, officer or other agent of the covered entity or business associate knows or should know by exercising reasonable diligence of the breach.

Since the 60 days is the outer limit for notification, if the full 60 day window is used, the covered entity or business associate involved in the breach must be prepared to justify their reasons for not providing notification of the breach sooner. However, notice of a breach may be delayed provided that notification would hinder a criminal investigation and/or injure national security (as determined by a law enforcement official). Covered entities may delegate responsibility for breach notifications to a business associate provided the business association agreement provisions mandate that the business associate has the same obligations that that covered entity has.

For business associates that discover a breach, the business associate must notify the covered entity of the breach or potential breach and the identity of all individuals affected or potentially affected. For covered entities, notification must be made to individuals whose unsecured protected health information has been accessed, acquired or disclosed or is reasonably believed to have been accessed, acquired or disclosed as a result of a security or privacy breach. In general, notification to affected individuals must be sent via first class mail. However, where a breach involves 10 or more individuals whose contact information is out-of-date or deficient, notification must be posted to the covered entity’s website or published in major print or broadcast media. For a breach that involves 500 or more individuals, the covered entity involved in the breach must also give notice to prominent media outlets in the applicable jurisdiction or state. However, the covered entity is not required to incur costs to print or run a media notice and media outlets are not obligated to print or run information about breaches when they receive notifications.

Notice of all breaches must be provided to the Secretary. If the breach affects 500 or more individuals, the covered entity involved in the breach must immediately notify the Secretary. For breaches that affect less than 500 individuals, the covered entity involved in the breach may notify the Secretary of any breaches on an annual basis.

**Q/A-16 How and what information must be contained in a notice of breach?**

The following methods of notice are appropriate:

* Written notice to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual).
* In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the Web site of the covered entity or notice in major print or broadcast media.
* In cases that the covered entity deems urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.
* Notice to prominent media outlets within the State or jurisdiction if a breach of unsecured PHI affects or is reasonably believed to affect more than 500 residents of that State or jurisdiction.
* Notice to the Secretary by covered entities immediately for breaches involving more than 500 individuals and annually for all other breaches.
* Posting by the Secretary on an HHS Web site of a list that identifies each covered entity involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed.

To the extent possible, all notices must contain:

* A brief description of what happened, including the date of the breach and the date of the discovery of the breach (if known);
* A description of the types of unsecured protected health information involved in the breach (e.g., social security number, date of birth);
* The steps individuals should take to protect themselves from potential harm as a result of the breach;
* A brief description of what the entity involved is doing to investigate the breach, to mitigate losses and to protect against further breaches; and
* Contact procedures for individuals to ask questions or receive additional information, including a toll-free telephone number and an e-mail address, web site or postal address.

**Q/A-17 Are there any exceptions to the required notice of a breach?**

On April 17, 2009, HHS issued proposed information security guidance specifying how covered entities may safeguard PHI and personal health records (PHRs) in such a manner that renders each unusable, unreadable, or indecipherable to unauthorized individuals, thereby relieving those covered entities subject to the HITECH Act from its breach notification requirements.

HHS’s proposed guidance specifies two methods for securing PHI and PHRs in a manner that would avoid application of the HITECH Act’s breach notification provisions. First, the proposed guidance provides that PHI and PHRs will be deemed unusable, unreadable or indecipherable if the information has been encrypted, provided the encryption key has not also been breached. Encryption must comply with the HIPAA Security Rule’s provisions, which define encryption as “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.”

HHS’s proposed guidance provides two specific examples of encryption that are deemed to meet this standard: (1) for data at rest, encryption consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111; and (2) for data in transit, encryption that complies with Federal Information Processing Standard 140-2. The proposed guidance provides that PHI and PHRs will be deemed unusable, unreadable or indecipherable if media on which they are stored or recorded have been destroyed by one of the following methods: (1) paper, film or other hard copy media have been shredded or destroyed such that PHI and PHRs cannot be read or reconstructed; and (2) electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88 such that PHI and PHRs cannot be retrieved.

The guidance acknowledges that use of the technologies and methodologies described therein are not required but, if used, “create the functional equivalent of a safe harbor” with respect to the breach notification provisions contained in the HITECH Act. The proposed guidance also indicates that any other applicable requirements, such as mitigation requirements contained in the HIPAA Privacy Rule and state breach notification laws, must be followed to the extent applicable, regardless of adherence to the guidance.

While these standards have not been enacted at this point, they provide some information on what information will be contained in the final guidance.

**Q/A-18 What are the penalties for non-compliance?**

The Secretary may conduct periodic audits of covered entities and business associates to ensure compliance with HIPAA Rules. The Secretary is also authorized to utilize civil enforcement provisions even if the action in question violated the criminal provisions, provided no criminal conviction is associated with the conduct.

The Secretary is required to impose civil penalties if a violation is due to willful neglect and to formally investigate any complaint if a preliminary investigation indicates the potential of violation due to willful neglect. For cases involving violations where the individual did not know of the violation or where the individual would not have known of the violation by exercising reasonable diligence, corrective action rather than penalty may still be used.

Under HIPAA Rules, criminal enforcement for certain HIPAA violations is not limited to covered entities. For purposes of criminal enforcement provisions, ARRA provides that “a person (including an employee or other individual)” is considered to have obtained or disclosed individually identifiable health information in violation of HIPAA if such information is maintained by a covered entity and the individual obtained or disclosed such information without authorization.

Civil penalties for violation of the HIPPA rules are broken into tiers which provide for the penalty amount to be based on the nature and extent of the violation and the harm caused by the violation:

* Tier 1 applies where the violator did not know of the violation, and would not have known even with reasonable diligence of the violation. In such circumstances, the penalty is not less than $100 per violation, and not more than $50,000 per violation of identical requirement or prohibition within the same year.
* Tier 2 applies where the violation was due to reasonable cause rather than willful neglect. In such circumstances, the penalty is not less than $1,000 per violation, and not more than $50,000 per violation. of an identical requirement or prohibition within the same calendar year
* Tier 3 applies where the violation was due to willful neglect but the violation was corrected within 30 days of the violation. The penalty is not less than $10,000 per violation, and not more than $50.000 per violation of an identical requirement or prohibition within the same calendar year.
* Tier 4 applies where the violation was due to willful neglect and the violation was not corrected within 30 days of the violation. The penalty is not less than $50,000 per violation of an identical requirement or prohibition within the same calendar year.

A penalty for violations of the same tier will not exceed $1.5 million in a calendar year, but multiple violations of multiple requirements may be subject to the maximum penalty of $1.5 million times the number of requirements violated.

The maximum penalty amount will not necessarily be levied in all cases. There will be a determination based on factors including but not limited to: the nature and extent of the violation; the harm resulting from the violation; prior offenses or compliance of the entity involved; and the financial condition of the entity.

In the case of a breach that affects multiple individuals, the number of violations will be based on the number of individuals affected. In the case of a breach that is continuous over a period of time, the number of violations will be based on the number of days that the entity did not have the breached information sufficiently protected. In the case of a breach involving violations of two or more provisions, a separate calculation may be made for each provision breached.

Increased penalty amounts may be levied if the violation due to willful neglect is not corrected within 30 days. Under the final regulations, for violations involving willful neglect, additional penalties may be assessed if the entity does not correct within 30 days. The 30 days begins to run when the entity first has actual or constructive knowledge of a violation due to willful neglect.

**Summary of New HIPAA Final Privacy Regulations**

On January 17, 2013, the Department of Health and Human Services released final regulations which provided sweeping changes to the rules update under privacy, security, enforcement, and breach notification requirements of the Health Insurance Portability and Accountability Act (“HIPAA”), the Health Information Technology for Economic Health (“HITECH”) and Genetic Information Nondiscrimination Act (“GINA”) Group health plans and business associates are required to comply with the regulations by September 23, 2013, unless otherwise stated in the regulations. With respect to the requirements on breaches of unsecured Protected Health Information (“PHI”), group health plans must still comply with the September 23, 2009 date. The following is a summary of the important changes under these final regulations.

1. **Business Associates**

Definition of Business Associate

Several updates and clarifications to the HIPAA definition of Business Associates (“BA”) have been included.

A person or entity becomes a BA by (i) meeting the definition of a BA and (ii) creating, receiving, maintaining, or transmitting PHI on behalf of a covered entity. Whether or not such person or entity has contracted with the covered entity and/or has entered into a Business Associate Agreement (“BAA”) is not determinative. Additionally, the type of PHI involved in the transaction does not matter – information is considered PHI if the information is related to a covered entity.

The definition of BAs also include:

* health information organizations;
* e-prescribing gateways;
* other entities that provide data transmission services with respect to PHI to a covered entity and that require routine access to PHI;
* entities that offers a personal health record to one or more individuals on behalf of a covered entity; and
* entities that maintain PHI, whether or not the entities actually review the PHI.

Subcontractors of BAs

The HIPAA’s BA provisions also apply to BAs’ subcontractors (persons or entities that provide services to a BA which involves PHI to fulfill its contractual duties) if the subcontractors create, receive, maintain, or transmit PHI on behalf of BAs. Group health plans are not required to enter into Business Associate Agreements (“BAAs”) with subcontractors, but the BAA must contain provisions that BAs will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same HIPAA restrictions, conditions, and requirements that apply to the BA.

Additional Clarifications Regarding Bas

* Banking and financial institutions are not BAs with respect to payment process activities, as identified in § 1179 of HIPAA, but if the bank or financial institution’s scope of activities exceeds the payment process activities, it will be considered a BA.
* Patient safety activities were added to the list of functions that may be undertaken as a BA and were added to the definition of health care operations.
* An insurer of a health plan product or insurance policy that is purchased by a covered entity is not a BA of the covered entity just by providing the insurance or product. In order to be considered a BA, the insurer must perform a function that involves PHI.

Direct Liability

BAs are now directly liable for complying with certain HIPAA privacy and security rules:

* Impermissible use and disclosure of PHI
* Failure to provide breach notification to a covered entity
* Failure to disclose PHI when required
* Failure to provide access to electronic PHI to an individual, his/her designee or a covered entity
* Failure to provide to a covered entity an accounting of disclosures
* Failure to comply with HIPAA security rules contained in 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, and 164.314
* Failure to comply with the requirements relating to policies, procedures and documentation requirements of 45 C.F.R. § 164.316
* Failure to establish BAAs with subcontractors

1. **Business Associate Agreements (“BAA”)**

All Business Associate Agreements must be amended to include:

* Provisions requiring BAs to comply with the HIPAA security rule
* Provisions requiring BAs to report breaches involving unsecured PHI to covered entities
* Provisions requiring BAs to obtain satisfactory assurances that subcontracts agree to comply with the underlying BAA’s conditions and restrictions as applied to PHI

Additionally, the final regulations do remove the requirement that BAAs include a provision that required covered entities to report to the Department of Health and Human Services when a BA was out-of-compliance, was not able to cure the breach, and it was not possible to terminate the BAA between the covered entity and the BA.

The final regulations also provide for a “grandfathered” transition period for updating BAAs. If a HIPAA-compliant BAA was in effect prior to January 25, 2013 and is not renewed or modified between March 26, 2013, and September 23, 2013, the covered entity and BA may continue to operate under the current BAA for up to **one year past** the final regulation compliance date. That is, the BAA does not have to be amended until the earlier of: (1) the date the BAA is renewed or modified on or after September 23, 20133 or (2) September 22, 2014. This extension for compliance also applies to BAAs that contain automatic renewal provisions.

1. **Notice of Privacy Practices**

Notices of Privacy Practices (“NPP”) must now be amended to include the following information (in addition to the existing HIPAA requirements):

* A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization;
* A statement that an individual has a right to or will receive notifications of breaches of his or her unsecured PHI;
* If the plan intends to use or disclose PHI for underwriting purposes, a statement that the plan is prohibited from using or disclosing PHI that is genetic information of an individual for such purposes; and
* If the plan intends to contact an individual to raise funds for the plan, a statement regarding fundraising communications and an individual’s right to opt out of receiving such communications.

For group health plans that post the NPP on their websites, the final regulations require that these plans must prominently post the changes or a revised Notice of Privacy Practices on websites by the September 23, 2013 compliance date; and provide the revised Notices of Privacy Practices, or information about the changes and how to obtain the revised Notices of Privacy Practices, in their next annual mailings to individuals then covered by the plans, such as at the beginning of the plan year or during open enrollment.

1. **Breach Notification**

Definition of Breach

The definition of what constitutes a “breach” has been changed. Breach is now defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. However, the final regulations made no change to the existing exceptions to the definition of breach.

With the change to the definition of breach, the previously used risk of harm standard has been replaced with the rule that, unless one of the enumerated exceptions is applicable, an unauthorized use or disclosure of PHI is presumed to be a breach. To overcome the presumption, a covered entity or BA must show that there is a “low probability that the PHI has been compromised.”

In support of this, the final regulations also identified four factors that must be evaluated by a covered entity or BA when determining whether PHI has been compromised:

1. What is the nature and extent of the PHI involved in the potential breach,
2. Who was the unauthorized user or recipient of the PHI,
3. Was the PHI actually received or viewed by the unauthorized user or recipient, and
4. To what extent has the breached PHI been mitigated.

The above four factors of the risk assessment are not determinative. Other factors may also need to be considered, depending on the individual circumstances of the breach. The risk assessment performed and conclusions reached by the covered entity or BA should be documented.

Additionally, the definition of breach has been changed by removing the exception for limited data sets that do not contain any dates of birth and zip codes.

Notice Requirements

Only a few changes have made to o the breach notice requirements. These include:

* A covered entity must notify the Department of Health and Human Services of all breaches affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breach was discovered rather than when the breach occurred
* Covered entities may delegate responsibility for breach notifications to a BA provided the BAA provisions provide that the BA has the same obligations that the covered entity has under the final regulations
* The plan is not required to incur costs to print or run a media notice, when it must provide notice of a breach to the media (i.e., breaches involving 500+ individuals in a state or jurisdiction). Also, media outlets are not obligated to print or run information about breaches when they receive notifications about them.
* The plan must provide notice within 60 days after the plan discovers the breach (rather than 60 days after the breach occurred), when the notice of a breach affects fewer than 500 individuals.

For this purpose, discovery means the first day on which an employee, officer other agent of the covered entity or BA knows or should know by exercising reasonable diligence of the breach.

1. **Use and Disclosure of PHI**

Use and Disclosure of PHI for Marketing Purposes

Individuals must now provide authorizations for certain communications where covered entities use or disclose PHI and receive financial remuneration for making the communications from a third party whose product or service is being marketed.

The Department of Health and Human Services clarified that remuneration related to marketing communications must be from or on behalf of the entity whose product or service is being described as well as it being in exchange for making the communication itself. Even if a BA, rather than the covered entity, receives the payment, the communication would be considered a marketing communication.

A covered entity must obtain an individual’s authorization prior to using or disclosing PHI about the individual for marketing purpose other than the following:

* treatment or health care operations activities that are made face-to-face, or
* The provision of a promotional gift of nominal value to the individual.

The definition of marketing does not include:

* refill reminders or other communications about a drug that is currently prescribed for the individual, as long as the financial remuneration received is reasonably related to the cost of making the communication
* promoting health in general, not promoting a specific product or service
* information related to government and government-sponsored programs

Use of PHI for Fundraising Purposes

If a covered entity (or a BA), uses an individual’s PHI for purposes of raising funds, the communication’s recipient must be provided with a “clear and conspicuous” opportunity to opt out of receiving any further fundraising communications. The method for “opting out” is left up to the covered entity to determine. However, the opt-out process may not create undue burden or more than nominal cost for the individual.

The use and disclosure of the following types of PHI can be used for fundraising:

* Demographic information relating to an individual,
* Dates of health care provided to an individual,
* Department of service information,
* Outcome information, and
* Health insurance status

However, the rule that when using PHI to make fundraising communications, the minimum necessary standard still applies and only the minimum amount of PHI necessary to accomplish the intended purpose may be used or disclosed is still applicable.

Prohibition on Sale of PHI

A covered entity or BA is only allowed to receive remuneration (direct or indirect) in exchange for the disclosure of PHI if an individual’s authorization is granted. The authorization must state that direct or indirect remuneration is being received in exchange for the PHI, unless an allowed exception applies. Sale of protected health information is defined as the disclosure of PHI by a covered entity or BA, where the entity or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. The exceptions to the prohibition of the sale of PHI are:

* For public health purposes
* For treatment of the individual and payment purposes.
* For the sale, transfer, merger or consolidation of all or part of a covered entity and for related due diligence purposes if the recipient of the PHI is or will become a covered entity
* For research purposes, if the remuneration is cost-based
* Services rendered by a BAA under a BAA at the specific request of the covered entity, as long as the remuneration is cost-based
* Providing an individual with access to the individual’s PHI
* As required by law
* For any other purpose permitted by HIPAA

Other Changes to Use and Disclosure of PHI

PHI stored in electronic devices such as photocopiers, fax machines, and other devices is now subject to the Privacy and Security Rules.

Covered entities are now permitted to disclose decedents’ PHI to family members and others who were involved in decedents’ care or payment for care prior to death, unless the covered entities know that such disclosure would be inconsistent with the decedents’ prior expressed wishes. If such disclosure will be allowed by the covered entity, it must be limited to PHI relevant to the family members or other persons’ involvement in the decedents’ health care or payment for health care.

Additionally, a covered entity may disclose proof of immunizations to schools in states that have laws that require the school to have such information prior to admitting a student. Although written authorization for the disclosure is not required, it is encouraged.

1. **Changes to Patient Rights**

Right to Access Protected Health Information

If individuals requests electronic copies of PHI that are maintained electronically in one or more designated record sets, covered entities must now provide access to the information in the electronic form and format requested by the individual, if readily producible.

If not readily producible, covered entities must provide the PHI in a readable electronic form and format which is agreed to by the covered entities and the individual, such as Word, Excel, text, HTML, or text-based PDF. Additionally, the final regulations provide:

* + A plan must respond to such a request within 30 days of the request, with a one-time 30-day extension when necessary. If a plan takes the 30-day extension, it must provide written notice to the individual of the reasons for delay and the expected date for completing the request.
  + If an individual declines any readily producible electronic format, the plan must provide a hard copy as an option.
  + A plan can require individuals to make these requests for PHI in writing.
  + A plan is not required to scan paper documents to provide electronic copies.
  + If requested, a plan must transmit the copy of PHI directly to another person designated by the individual who is the subject of the PHI. If an individual directs the plan to send a copy of PHI to another person, the request must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI. The plan must implement reasonable policies and procedures to verify the identity of any person who requests PHI and implement reasonable safeguards to protect the information used or disclosed.
  + With respect to PHI from an electronic health record in electronic form, a plan cannot charge more than labor costs in responding to an individual’s request. These costs may include skilled technical staff time spent to create and copy the electronic file or time spent preparing and explanation or summary of the PHI, if appropriate. A plan also can charge for the cost of supplies (such as CDs or USB drives) for creating the copy of PHI, if the individual requests the electronic copy on portable media, and associated postage.

Restrictions on Disclosures by Health Plans

The processes surrounding the requirement that covered entities must comply with an individual’s request to restrict disclosure of PHI to a health plan if certain conditions are met have been clarified. Under the final regulations:

* Health providers are not required to maintain separate medical records when a request to restrict disclosure is made, but they are required to use some method to identify which portions of the medical records are subject to the restriction request.
* If a restriction is requested where payment is pending, health providers must either make reasonable efforts at resolving the payment issues before disclosing PHI or should request payment in full at the time of the requested restriction.
* If an individual requests a restriction, it is the individual’s responsibility – not the health providers – to notify any other providers who might be impacted.
* HMO contractual requirements do not negate a provider’s responsibility to adhere to a request to restrict disclosures.

1. **Penalties**

Consequences of Noncompliance

The final regulations significantly increase covered entities and BAs potential exposure to civil monetary penalties and creates uncertain risk. First, covered entities and BAs will be liable under federal common law of the acts of their agents.

Next, the assessment of penalties will be left to fact specific analyses and the Department of Health and Human Services’ discretion. There are four categories of HIPAAA violations that reflect increasing levels of culpabilities accompanied by four tiers of significantly increased monetary penalties. These include:

Tier 1: For violations in which it is established that the covered entity of BA did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than $100 or more than $50,000 for each violation

Tier 2: For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than $1000 or more than $50,000 for each violation

Tier 3: For a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation

Tier 4: For a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than $50,000 for each violation

A penalty for violations of the same tier will not exceed $1.5 million in a calendar year, but multiple violations of multiple requirements may be subject to the maximum penalty of $1.5 million times the number of requirements violated.

The maximum penalty amount will not necessarily be levied in all cases. There will be a determination based on factors including but not limited to: the nature and extent of the violation; the harm resulting from the violation; prior offenses or compliance of the entity involved; and the financial condition of the entity.

The final regulations provide insight into the application of penalties. In the case of a breach that affects multiple individuals, the number of violations will be based on the number of individuals affected. In the case of a breach that is continuous over a period of time, the number of violations will be based on the number of days that the entity did not have the breached information sufficiently protected. In the case of a breach involving violations of two or more provisions, a separate calculation may be made for each provision breached.

Increased penalty amounts may be levied if the violation due to willful neglect is not corrected within 30 days. Under the final regulations, for violations involving willful neglect, additional penalties may be assessed if the entity does not correct within 30 days. The 30 days begins to run when the entity first has actual or constructive knowledge of a violation due to willful neglect.

1. **GINA Implementation**

The Department of Health and Human Services’ proposals have be adopted to:

* Provide that genetic information is considered health information for purposes of HIPAA privacy rules and therefore subject to HIPAA privacy requirements;
* Prohibit all health plans that are subject to HIPAA privacy rules from using or disclosing PHI that is genetic information for underwriting purposes (except with regard to insurance issuers of long term care policies);
* Revise the HIPAA requirements relating to Notices of Privacy Practices for health plans that perform underwriting;
* Make conforming changes to definitions and other provisions of the HIPAA privacy rules; and
* Make technical corrections.

For a copy of the final regulations, please click on the link below:

<https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>

**HIPAA PRIVACY POLICY**

Introduction

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Employer”) sponsors the following group health plans:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the above plans are considered to be “covered entities.” For purposes of this Privacy Policy, the plans listed above are referred to collectively and singularly as the “Plan.” Members of the Employer’s workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan; or (2) on behalf of the Employer, for administrative functions of the Plan.

HIPAA as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its implementing regulations restrict the Employer’ ability to use and disclose protected health information (PHI).

*Protected Health Information.* Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a 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.

It is the Employer’s policy to comply fully with HIPAA’s requirements for the privacy of PHI. To that end, all members of the Employer’s workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Employer’s more detailed use and disclosure procedures, the Employer’s workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. The term “employee” includes all of these types of workers. Additionally, any subcontractors that provide services to the Employer, which involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Employer to fulfill its contractual duties, must comply fully with HIPAA’s requirements.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Employer reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan or the Employer. This Policy does not address requirements under other federal laws or under state laws. To the extent that this policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

**Plan’s Responsibilities as Covered Entity**

**I. Privacy Official and Contact Person**

The Employer shall designate the individual responsible for the human resource function of the Employer as the Privacy Officer.

The Privacy Official 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 Employer’s more detailed use and disclosure procedures. The Privacy Official will also appoint those employees who will serve as the contact persons for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules regarding business associates, including the requirement that the Plan have a HIPAA-compliant Business Associate Agreement in place with all business associates. The Privacy Official shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and this Privacy Policy.

**II. Workforce Training**

It is the Employer’s policy to train all members of its workforce on its privacy policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plan in compliance with HIPAA.

**III. Administrative, Technical and Physical Safeguards and Firewall**

The Employer will establish on behalf of the Plan appropriate administrative, technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA’s requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. See the Plan’s Privacy Use and Disclosure Procedures. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA’s privacy rules.

**IV. Privacy Notice**

The Privacy Official is responsible for developing and maintaining a notice of the Plan’s privacy practices that describes:

* the uses and disclosures of PHI that may be made by the Plan;
* the individual’s rights under the HIPAA privacy rules;
* the Plan’s legal duties with respect to the PHI; and
* other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Employer will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Employer’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:

* at the time of an individual’s enrollment in the Plan;
* to a person requesting the notice; and
* within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

**V. Complaints**

The Privacy Officer will be the Plan’s contact person for receiving complaints.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan’s privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

**VI. Sanctions for Violations of Privacy Policy**

Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Employer’s discipline policy, up to and including termination.

**VII. Mitigation of Inadvertent Disclosures of Protected Health Information**

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual’s PHI in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a disclosure of protected health information, either by an employee or a business associate the employee or the business associate, that is not in compliance with this policy or HIPAA, the employee should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

**VIII. 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 under the Plan.

**IX. Plan Documents**

Plan documents shall include provisions to describe the permitted and required uses and disclosures of PHI by the Employer for plan administrative purposes or other permitted purposes. Specifically, Plan documents shall require the Employer 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 Plan agree to the same restrictions and conditions that apply to the Employer;
* not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
* report to the privacy Officer any use or disclosure of the information that is inconsistent with the permitted use or disclosure and, if necessary, report such use or disclosure to the Department of Health and Human Services (HHS),as required by HITECH and subsequent regulations;
* make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with HIPAA privacy rules;
* make the Employer’s internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request;
* if feasible, return or destroy all PHI received from the Plan that the Employer still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible: and
* provide access to electronic PHI to an individual or his/her designee.

The Plan documents must also require the Employer to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Employer agree to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

**X. Documentation**

The Plan’s privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. 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 promptly be documented.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual’s privacy rights.

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.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Plan must maintain such documentation for at least six years.

**Policies on Use and Disclosure of PHI**

**I. Use and Disclosure Defined**

The Employer and the Plan 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 benefits department of the Employer, or by a Business Associate (defined below) of the Plan.
* *Disclosure.* For information that is PHI, 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 the Human Resources Department of the Employer, or not a Business Associate (defined below) of the Plan.

**II. Workforce Must Comply With Plan’s Policy and Procedures**

All members of the Employer’s workforce (described at the beginning of this Policy and referred to herein as “employees”) who has access to Plan PHI must comply with this Policy and with the Plan’s more detailed use and disclosure procedures, which are set forth in a separate document.

**III. Access to PHI Is Limited to Certain Employees**

The following employees (“employees with access”) have access to PHI:

* Any employee who performs functions directly on behalf of the Plan; and
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*inset title(s) of anyone else with access for administrative functions*] who has access to PHI on behalf of the Business Associate for its use in “plan administrative functions” of the covered entities.

The same employees may be named or described in both of these two categories. These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and any associated procedures.

**IV. Permitted Uses and Disclosures for Plan Administration Purposes**

The Plan may disclose to the Employer for its use the following: (a) de-identified health information relating to plan participants; (b) Plan enrollment information; (c) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under the Plan or for modifying, amending, or terminating the Plan; or (d) PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Plan may disclose PHI to the following employees who have access to use and disclose PHI to perform functions on behalf of the Plan or to perform plan administrative functions (“employees with access”):

* Any employee who performs functions directly on behalf of the Plan; and
* Any other employee who has access to PHI on behalf of the Employer for its use in “plan administrative functions.”

The same employees may be named or described in both of these two categories. These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the more detailed use and disclosure procedures.. For purposes of this Policy, “plan administrative functions” include the payment and health care operation activities described in this section of this Policy.

**V. Permitted Uses and Disclosures: Payment and Health Care Operations**

The Plan may disclose to the Employer for the Plan’s own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

*Payment.* Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan’s responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

* eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
* risk adjusting based on enrollee status and demographic characteristics;
* billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing; and
* any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan’s own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity’s quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

*Health Care Operations.* Health care operations means any of the following activities to the extent that they are related to Plan administration:

* conducting quality assessment and improvement activities;
* reviewing health plan performance;
* underwriting and premium rating;
* conducting or arranging for medical review, legal services and auditing functions;
* business planning and development;
* business management and general administrative activities;
* to de-identify the information in accordance with HIPAA Rules as necessary; and
* any other payment activity permitted by the HIPAA privacy regulations.

**VI. No Disclosure of PHI for Non-Health Plan Purposes**

PHI may not be used or disclosed for the payment or operations of the Employer’s “non-health” benefits (e.g., disability, workers’ compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in “Disclosures Pursuant to an Authorization”) or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

**VII. Mandatory Disclosures of PHI: to Individual and HHS**

A participant’s PHI must be disclosed as required by HIPAA in three situations:

* The disclosure is to the individual who is the subject of the information (see the policy for “Access to Protected Information and Request for Amendment” that follows);
* The disclosure is required by law, or
* The disclosure is made to HHS for purposes of enforcing of HIPAA.

**VIII. Other Permitted Disclosures of PHI**

PHI may be disclosed in the following situations without a participant’s authorization, when specific requirements are satisfied. The requirements include prior approval of the Employer’s Privacy Official. Permitted are disclosures—

* about victims of abuse, neglect or domestic violence;
* for treatment purposes;
* for judicial and administrative proceedings;
* for law enforcement purposes;
* for public health activities;
* for health oversight activities;
* about decedents;
* for cadaveric organ, eye or tissue donation purposes;
* for certain limited research purposes;
* to avert a serious threat to health or safety;
* for specialized government functions; and
* that relate to workers’ compensation programs.

**IX. 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.

**X. 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 HHS;
* uses or disclosures required by law; and
* uses or disclosures required to comply with HIPAA.

*Minimum Necessary When Disclosing PHI.* The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

*Minimum Necessary When Requesting PHI.* The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

**XI. Disclosures of PHI to Business Associates**

Employees may disclose PHI to the Plan’s business associates and allow the Plan’s business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan 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 Official and verify that a business associate contract is in place.

*Business Associate* is an entity that:

* performs or assists in performing a Plan 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;
* health information organizations;
* e-prescribing gateways;
* other entities that provide data transmission services with respect to PHI and require routine access to PHI;
* entities that offer a personal health record to one or more individuals on behalf of a covered entity; or
* entities that maintain PHI, whether or not the entities actually review the PHI.

**XII. Disclosures of De-Identified Information**

The Plan may freely use and disclose de-identified information in accordance with HIPAA privacy regulations. 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 business associate can determine that information is de-identified: either by professional statistical analysis, or by removing specific identifiers.

**XIII. Physical Access Controls/Guidelines to Guard PHI**

The Employer will maintain strict physical access controls to its information systems at all times and under all conditions. This includes the physical security of electronic and paper data.

The Employer will terminate access to information systems and other sources of PHI, including access to rooms or buildings where PHI is located, when an employee, agent or contractor ends his/her employment or engagement. The Employer will terminate access to specific types of PHI when the status of any member of the workforce no longer requires access to those types of information.

**Cleaning personnel:**

Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets or rooms before cleaning personnel enter an area. When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area and a supervisor must be present.

**Computer Screens:**

Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed. Computerdisplays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time. The period of time will be determined by the Compliance Official. Wherever practicable, reverting from the screen saver to the display of data will require a password. Computer screens left unattended for longer periods of time will log off the user. The period of time will be determined by the Privacy Official.

**Conversations:**

Conversations concerning individual care or other PHI must be conducted in a way that reduces the likelihood of being overheard by others. Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

**Copying medical records and other PHI:**

When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

**Desks and countertops:**

Provider reports and other documents which may display identifiers and other “keys” to information should be placed face down on counters, desks, and other places where individuals or visitors can see them. Wherever it is reasonably possible to do so, medical reports and other documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers or other means to secure PHI during periods when the area is left unattended. In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

**Disposal of paper with PHI:**

Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

**Home office:**

Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

**Key policy:**

The Privacy Official will develop a list of which personnel, by job title, may have access to which keys. This includes keys to storage cabinets, storage rooms and buildings. All keys must be signed out. Keys must be surrendered upon termination ofemployment. The Privacy Official will ensure that locks are changed whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

**Phones or Laptops:**

The privacy and security policies apply to any PHI that is stored on a phones or laptop. Users of PDAs and laptops are responsible for assuring that the PHI on their devices is kept secure and private. Any loss or theft of a phone or laptop thought to contain PHI must be reported to the Compliance Official immediately. Users of phones who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords).

**Printers and Fax Machines:**

Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed.

**Records carried from one building to another:**

When PHI is carried from one building to another, it must be signed out and signed in. When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

**Record Storage:**

Areas where records and other documents that contain PHI are stored must be secure. Wherever reasonably possible, the PHI will be stored in locking cabinets. Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision.

**Workforce Vigilance:**

All members of the workforce are responsible for watching for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or to the Privacy Official (example of a breach: individual or visitor looking through PHI left on a counter).

**Visitors:**

Visitors to areas where PHI is being used must be accompanied by a member of the Employer’s workforce.

**XIV. Breach Notification Requirements**

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

**Policies on Individual Rights**

**I. Access to PHI and Requests for Amendment**

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

*Designated Record Set* is a group of records maintained by or for the Plan that includes:

* the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
* other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

**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;
* pursuant to an authorization;
* to persons involved in the patient’s care or other notification purposes;
* to correctional institutions or law enforcement when the disclosure was permitted without authorization;
* as part of a limited data set;
* for specific national security or law enforcement purposes; or
* disclosures that occurred prior to the compliance date.

The Plan shall respond to an accounting request within 60 days. If the Plan 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). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

**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 the Employer, the requests are reasonable.

However, the Employer shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

**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 Plan’s’ policy to attempt to honor such requests if, in the sole discretion of the Employer, the requests are reasonable. The Plan is charged with responsibility for administering requests for restrictions and shall communicate any restrictions to the

Privacy Official.

**HIPAA PRIVACY USE AND DISCLOSURE PROCEDURES**

**Introduction**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Employer”) sponsors the following health plans:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For purposes of these procedures the plans listed above are referred to collectively and singularly as the “Plan.” Members of the Employer's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Employer, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Employer's ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a 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.

It is the Employer's policy to comply fully with HIPAA's requirements. To that end, all members of the Employer's workforce who have access to PHI must comply with these Use and Disclosure Procedures. For purposes of these Use and Disclosure Procedures and the Employer's separate privacy policy,the Employer's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. The term "employee" includes all of these types of workers. Additionally, any subcontractors that provide services to the Business Associate which involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Business Associate to fulfill its contractual duties, must comply fully with HIPAA’s requirements.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these Use and Disclosure Procedures. The Employer reserves the right to amend or change these Use and Disclosure Procedures at any time (and even retroactively) without notice. To the extent these Use and Disclosure Procedures establish requirements and obligations above and beyond those required by HIPAA, these Use and Disclosure Procedures shall be aspirational and shall not be binding upon the Employer. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

**Procedures for Use and Disclosure of PHI**

**I. Use and Disclosure Defined**

The Employer and the Plan 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 human resources department of the Employer, or by a Business Associate (defined below) of the Plan.
* Disclosure. For information that is PHI, 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 the human resources department of the location(s) of the Employer.

**II. Workforce Must Comply With Employer's Policy and Procedures**

All members of the Employer's workforce (described at the beginning of these Use and Disclosure Procedures and referred to herein as "employees") must comply with these Use and Disclosure Procedures and the Employer's separate privacy policy.

**III. Access to PHI Is Limited to Certain Employees**

The following employees ("employees with access") have access to PHI:

* Those employees who perform functions directly on behalf of the Plan, and
* Any other employee who has access to PHI on behalf of the Employer for its use in “plan administrative functions”.

These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) except in accordance with these Use and Disclosure Procedures.

**IV. Permitted Uses and Disclosures of PHI: Payment and Health Care Operations**

**Definitions**

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

* eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
* risk adjusting based on enrollee status and demographic characteristics; and
* billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

* conducting quality assessment and improvement activities;
* reviewing health plan performance;
* underwriting and premium rating;
* conducting or arranging for medical review, legal services and auditing functions;
* business planning and development;
* business management and general administrative activities;
* to de-identify the information in accordance with HIPAA Rules as necessary to perform required services.

**Procedure**

* Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations. An employee may use and disclose a Plan participant's PHI to perform the Plan’s own payment activities or health care operations.
* Disclosures must comply with the "Minimum-Necessary” Standard. (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."
* Disclosures for Another Entity's Payment Activities. An employee may disclose a Plan participant's PHI to another covered entity or health care provider to perform the other entity's payment activities. These disclosures will be made according to procedures developed by the Privacy Official.
* Disclosures for Certain Health Care Operations of the Receiving Entity. An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are made according to procedures developed by the Privacy Official.
* The disclosure must be approved by the Privacy Official.
* Disclosures must comply with the “minimum-Necessary Standard.”
* Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”
* Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, an employee may not use a participant's PHI for the payment or operations of the Employer's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow the steps provided by the Privacy Official.
* Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. **Employees shall not attempt to draft authorization forms.** All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Official.
* Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official or his or her designated representative.

**V. Mandatory Disclosures of PHI: to Individuals and HHS**

**Procedure**

* Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."
* Request From HHS. Upon receiving a request from a HHS official for disclosure of PHI, the employee must take the steps established by the Privacy Official.
* Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

1. **Permissive Disclosures of PHI: for Legal and Public Policy Purpose**

**Procedure**

* Disclosures for Legal or Public Policy Purposes. An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made according to procedures established by the Privacy Official.
* The disclosure must be approved by the Privacy Official.
* Disclosures must comply with the "Minimum-Necessary Standard."
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

**Legal and Public Policy Disclosures Covered**

* Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:
* The individual agrees with the disclosure; or
* The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.
* For Judicial and Administrative Proceedings, in response to:
* An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); and
* A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.
* To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:
* Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
* Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
* Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.
* Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
* Information that constitutes evidence of criminal conduct that occurred on the Employer's premises.
* To Appropriate Public Health Authorities for Public Health Activities.
* To a Health Oversight Agency for Health Oversight Activities, as authorized by law.
* To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.
* For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.
* For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.
* To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.
* For Specialized Government Functions, including disclosures of an inmate’s PHI to correctional institutions and disclosures of an individual's PHI to an authorized federal Official for the conduct of national security activities.
* For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

**VII. Disclosures of PHI Pursuant to an Authorization**

**Procedure**

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

* Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
* Verify that the authorization form is valid. Valid authorization forms are those that:
* Are properly signed and dated by the individual or the individual's representative;
* Are not expired or revoked [the expiration date of the authorization form must be a specific date (such as July 1, 2010) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage)];
* Contain a description of the information to be used or disclosed;
* Contain the name of the entity or person authorized to use or disclose the PHI;
* Contain the name of the recipient of the use or disclosure;
* Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
* Contain a statement regarding the possibility for a subsequent re-disclosure of the information.
* All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

**VIII. Disclosure of PHI to Business Associates**

**Definition of Business Associate**

Business Associate is an entity or person who:

* performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or
* 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;

Such Business Associates include:

* a health information organization;
* an e-prescribing gateway;
* another entity that provides data transmission services with respect to PHI to a covered entity and that requires routine access to PHI;
* is an entity that maintains PHI for a covered entity, whether or not the entity actually reviews the PHI.

**Procedure**

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a "business associate" must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees must contact the Privacy Official and verify that a business associate contract is in place.

The following additional procedures must be satisfied:

* Disclosures must be consistent with the terms of the business associate contract.
* Disclosures must comply with the "Minimum-Necessary Standard." (Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum-necessary requirement, and each non-recurring disclosure must be approved by the Privacy Official.)
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

**IX. Requests for Disclosure of PHI From Spouses, Family Members, and Friends**

The Plan and Employer will not disclose PHI to family or friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI.

* If an employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."
* Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access."
* All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

1. **Disclosures of De-Identified Information**

**Definition of 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.

**Procedure**

* Obtain approval from the Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.
* The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

1. **Verification of Identity of Those Requesting Protected Health Information**

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

* Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:
* Request a form of identification from the individual. Employees may rely on a valid driver’s license, passport or other photo identification issued by a government agency.
* Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
* Make a copy of the identification provided by the individual and file it with the individual's designated record set.
* If the individual requests PHI over the telephone, ask for his or her social Security number.
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."
* Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:
* Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.
* Disclosures must be documented in accordance with the procedure "Documentation Requirements."
* Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, the following steps should be followed:
* Require a copy of a valid power of attorney or other documentation—requirements may vary state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Official.
* Make a copy of the documentation provided and file it with the individual's designated record set.
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."
* Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," the following steps should be followed to verify the official's identity and authority:
* If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
* If the request is in writing, verify that the request is on the appropriate government letterhead.
* If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
* Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Legal Department.
* Obtain approval for the disclosure from the Privacy Official.
* Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

**XII. Complying With the "Minimum-Necessary" Standard**

**Procedures for Disclosures**

* Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of business associates. Create a policy for each specific recurring disclosure that limits the amount disclosed to the minimum amount necessary to accomplish the purpose of the disclosure.
* For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

**Procedures for Requests**

* Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure and create a policy that limits each request to the minimum amount necessary to accomplish the purpose of the disclosure.
* For all other requests for PHI, contact the Privacy Official, who will ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

**Exceptions**

* 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 an individual authorization;
* Disclosures made to HHS;
* Uses or disclosures required by law; and
* Uses or disclosures required to comply with HIPAA.

1. **Documentation**

**Procedure**

* Documentation. Employees shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:
* “Notices of Privacy Practices" that are issued to participants;
* Copies of policies and procedures;
* Individual authorizations;
* When disclosure of certain PHI is made:
* the date of the disclosure;
* the name of the entity or person who received the PHI and, if known, the address of such entity or person;
* a brief description of the PHI disclosed;
* a brief statement of the purpose of the disclosure; and
* any other documentation required under these Use and Disclosure Procedures.

**Note:** The retention requirement only applies to documentation required by HIPAA. It does not apply to all medical records.

1. **Mitigation of Inadvertent Disclosures of PHI**

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, if you become aware of a disclosure of PHI, either by an employee of Plan or an outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

1. **Breach Notification Requirements**

Compliance: The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

**Procedures for Complying With Individual Rights**

Individual Rights: HIPAA gives individuals the right to access and obtain copies of their protected health information that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that individuals may request to have their PHI amended, and that they are entitled to an accounting of certain types of disclosures.

1. **Individual's Request for Access**

**"Designated Record Set" Defined**

Designated Record Set is a group of records maintained by or for the Employer that includes:

* the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
* other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

**Procedure**

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employee must take the following steps:

* Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
* Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. No request for access may be denied without approval from the Privacy Official.
* Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, information compiled during research when the individual has agree to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.
* Respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 -day period of the reasons for the extension and the date by which the Employer will respond.
* A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.
* Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
* Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.
* If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
* Charge a reasonable cost-based fee for copying, postage, and preparing a summary (but the fee for a summary must be agreed to in advance by the individual). This provision is not needed if the plan will not charge a fee.
* Disclosures must be documented in accordance with the procedure "Documentation Requirements."

**II. Individual's Request for Amendment**

**Procedure**

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, the employee must take the following steps:

* Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
* Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Official if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Official.
* Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official**.**
* Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the designated record set is accurate and complete without the amendment.
* Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.
* When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the unconnected information to the detriment of the individual.
* When an amendment request is denied, the following procedures apply:
* All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
* If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Employer's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

**III. Processing Requests for an Accounting of Disclosures of Protected Health Information**

**Procedure**

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

* Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
* If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.
* Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.
* The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to April 14, 2004. The accounting does not have to include disclosures made:
* to carry out treatment, payment and health care operations;
* to the individual about his or her own PHI;
* incident to an otherwise permitted use or disclosure;
* pursuant to an individual authorization;
* for specific national security or intelligence purposes;
* to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
* as part of a limited data set.
* If any business associate of the Plan has the authority to disclose the individual's PHI, then Privacy Officer shall contact business associate to obtain an accounting of the business associate's disclosures.
* The accounting must include the following information for each reportable disclosure of the individual's PHI:
* the date of disclosure;
* the name (and if known, the address) of the entity or person to whom the information was disclosed;
* a brief description of the PHI disclosed; and
* a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
* If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official for more guidance.
* Accountings must be documented in accordance with the procedure for "Documentation Requirements."

1. **Processing Requests for Confidential Communications**

**Procedure**

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

* Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
* Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
* The employee should take steps to honor requests.
* If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
* All confidential communication requests that are approved must be tracked.
* Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

**V. Processing Requests for Restrictions on Uses and Disclosures of Protected Health Information**

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for access to an individual's PHI, the employee must take the following steps: Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

* The employee should take steps to honor requests.
* If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
* All requests for limitations on use or disclosure of PHI that are approved must be tracked.
* All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions.
* Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

**BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement**,** is entered into as of \_\_\_\_\_\_\_\_, 2010, by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*Insert Name of Health Plan*] Health Plan *(*the “Plan” or “Covered Entity”); and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the "Business Associate").

**WITNESSETH:**

**WHEREAS**, the Covered Entity previously has entered into an agreement (the “Agreement”) with the Business Associate, whereby the Business Associate has agreed to provide certain services to the Plan;

**WHEREAS,** to provide such services to the Plan, the Business Associate must have access to certain protected health information ("Protected Health Information" or "PHI"), as defined in the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards") set forth by the U.S. Department of Health and Human Services (“HHS”) pursuant to the Health Insurance Portability and Accountability Act of 1996, ("HIPAA") and amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), part of the American Recovery and Reinvestment Act of 2009 (“ARRA”), the Genetic Information Nondiscrimination Act of 2008 (“GINA”) and the final regulations to such Acts promulgated in January 2013;

**WHEREAS,** to comply with the requirements of the Privacy Standards, the Covered Entity must enter into this Business Associate Agreement with the Business Associate.

**NOW, THEREFORE,** in consideration of the mutual covenants and agreements hereinafter contained, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound hereby, the parties hereto agree as follows:

**I. Definitions**

The following terms used in this Agreement shall have the same meaning as those terms in the Privacy Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Secretary, Subcontractor, and Use. If other terms are used, but not otherwise defined under this Business Associate Agreement, such terms shall then have the same meaning as those terms in the Privacy Rule.

1. ***Business Associate***. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103.
2. ***Covered Electronic Transactions.*** “Covered Electronic Transactions” shall have the meaning given the term “transaction”” in 45 CFR §160.103.
3. ***Covered Entity.*** “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103.
4. ***Electronic Protected Health Information.*** “Electronic Protected Health Information” shall have the same meaning as the term “electronic protected health information” in 45 CFR §160.103.
5. ***Genetic Information***. “Genetic Information” shall have the same meaning as the term “genetic information” in 45 CFR §160.103.
6. ***HIPAA Rules.*** “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
7. ***Individual.*** “Individual” shall have the same meaning as the term “individual” in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
8. ***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.
9. ***Protected Health Information (PHI).*** “Protected Health Information (PHI)” shall have the same meaning as the term “protected health information” in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of a Covered Entity pursuant to this Agreement.
10. ***Required By Law.*** “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR §164.103.
11. ***Secretary.*** “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.
12. ***Standards for Electronic Transactions Rule.*** “Standards for Electronic Transactions Rule” means the final regulations issued by HHS concerning standard transactions and code sets under the Administration Simplification provisions of HIPAA, 45 CFR Part 160 and Part 162.
13. ***Security Incident.*** “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR §164.304.
14. ***Security Rule.*** “Security Rule” shall mean the Security Standards and Implementation Specifications at 45 CFR Part 160 and Part 164, subpart C.
15. ***Subcontractor.*** “Subcontractor” shall have the same meaning as the term subcontractor in 45 CFR §160.103.
16. ***Transaction.*** “Transaction” shall have the meaning given the term “transaction” in 45 CFR §160.103
17. ***Unsecured Protected Health Information.*** “Unsecured Protected Health Information” shall have the meaning given the term “unsecured protected health information” in 45 CFR §164.402.

**II. Safeguarding Privacy and Security of Protected Health Information**

**(a) *Permitted Uses and Disclosures.*** The Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on the Covered Entity’s behalf or receives from the Covered Entity (or another business associate of the Covered Entity) and to request Protected Health Information on the Covered Entity’s behalf (collectively, “Covered Entity’s Protected Health Information”) only:

1. **Functions and Activities on** the **Covered Entity’s Behalf.** To perform those services referred in the attached services agreement.

**(ii) Business Associate’s Operations.** For the Business Associate’s proper management and administration or to carry out the Business Associate’s legal responsibilities, provided that, with respect to disclosure of the Covered Entity’s Protected Health Information, either:

1. The disclosure is Required by Law; or

(B) The Business Associate obtains reasonable assurance from any person or entity to which the Business Associate will disclose the Covered Entity’s Protected Health Information that the person or entity will:

(1) Hold the Covered Entity’s Protected Health Information in confidence and use or further disclose the Covered Entity’s Protected Health Information only for the purpose for which the Business Associate disclosed the Covered Entity’s Protected Health Information to the person or entity or as Required by Law; and

(2) Promptly notify the Business Associate (who will in turn notify the Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of the Covered Entity’s Protected Health Information was breached.

(C) To de-identify the information in accordance with 45 CFR 164.514(a) – (c) as necessary to perform those services required under the Agreement.

**(iii) Minimum Necessary.** The Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of the Covered Entity’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that the Business Associate will not be obligated to comply with this minimum-necessary limitation if neither the Business Associate nor the Covered Entity is required to limit its use, disclosure or request to the minimum necessary. The Business Associate and the Covered Entity acknowledge that the phrase “minimum necessary” shall be interpreted in accordance with the HITECH Act.

**(b) *Prohibition on Unauthorized Use or Disclosure.*** The Business Associate will neither use nor disclose the Covered Entity’s Protected Health Information, except as permitted or required by this Agreement or in writing by the Covered Entity or as Required by Law. This Agreement does not authorize the Business Associate to use or disclose the Covered Entity’s Protected Health Information in a manner that will violate Subpart E of 45 CFR Part 164 if done by the Covered Entity.

**(c) *Information Safeguards.***

**(i) Privacy of** the **Covered Entity’s Protected Health Information.** The Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of the Covered Entity’s Protected Health Information. The safeguards must reasonably protect the Covered Entity’s Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made to a use or disclosure otherwise permitted by this Agreement.

**(ii) Security of** the **Covered Entity’s Electronic Protected Health Information.** The Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that the Business Associate creates, receives, maintains, or transmits on the Covered Entity’s behalf as required by the Security Rule. The Business Associate will comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information to prevent use or disclosure of protected health information other than as provided for by the Agreement.

1. **No Transfer of PHI Outside United States**. The Business Associate will not transfer Protected Health Information outside the United States without the prior written consent of the Covered Entity. In this context, a “transfer” outside the United States occurs if Business Associate's workforce members, agents, or subcontractors physically located outside the United States are able to access, use, or disclose Protected Health Information.

**(iv) Policies and Procedures.** The Business Associate shall maintain written policies and procedures, conduct a risk analysis, and train and discipline of its workforce.

**(d) *Subcontractors and Agents.*** In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, the Business Associate will ensure that any of its Subcontractors and agents that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.,

**(e) *Prohibition on Sale of Records.*** As of the effective date specified by HHS in final regulations to be issued on this topic, the Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtained from the individual, in accordance with 45 CFR §164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under the HITECH Act.

**(f) Prohibition on Use or Disclosure of Genetic Information.** The Business Associate shall not use or disclose Genetic Information for underwriting purposes in violation of the HIPAA rules.

**(g) *Penalties For Noncompliance.*** The Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the privacy rule and security rule, under the HIPAA Rules, as amended by the HITECH Act.

**III. Compliance with Electronic Transactions Rule**

If the Business Associate conducts in whole or part Electronic Transactions on behalf of the Covered Entity for which HHS has established standards, the Business Associate will comply, and will require any Subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule. The Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

**IV. Obligations of the** **Covered Entity**

The Covered Entity shall notify the Business Associate of:

(a) Any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect the Business Associate’s use or disclosure of Protected Health Information;

(b) Any changes in, or revocation of, permission by the Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate’s use or disclosure of Protected Health Information; and

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

**V. Permissible Requests by** the **Covered Entity**

The Covered Entity shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

**VI. Individual Rights**

**(a) *Access.*** TheBusiness Associate will, within twenty-five (25) calendar days following the Covered Entity’s request, make available to the Covered Entity or, at the Covered Entity’s direction, to an individual (or the individual’s personal representative) for inspection and obtaining copies of the Covered Entity’s Protected Health Information about the individual that is in the Business Associate’s custody or control, so that the Covered Entity may meet its access obligations under 45 CFR §164.524. Effective as of the date specified by HHS, if the Protected Health Information is held electronically in a designated record Set in the Business Associate’s custody or control, the Business Associate will provide an electronic copy in the form and format specified by the Covered Entity if it is readily producible in such form. The Business Associate will provide an electronic copy in the form and format specified by the Covered Entity if it is readily producible in such format; if it is not readily producible in such format, the Business Associate will work with the Covered Entity to determine an alternative forma and format as specified by the Covered Entity to meet its electronic access obligations under 45 CFR 164.524.

**(b) *Amendment.*** TheBusiness Associate will, upon receipt of written notice from the Covered Entity, promptly amend or permit the Covered Entity access to amend any portion of the Covered Entity’s Protected Health Information in a designated record set as directed or agreed to by the Covered Entity, so that the Covered Entity may meet its amendment obligations under 45 CFR §164.526.

**(c) *Disclosure Accounting.*** The Business Associate will maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity’s obligations under 45 CFR §164.528.

**(i) Disclosures Subject to Accounting.** The Business Associate will record the information specified below (“Disclosure Information”) for each disclosure of the Covered Entity’s Protected Health Information, not excepted from disclosure accounting as specified below, that the Business Associate makes to the Covered Entity or to a third party.

**(ii) Disclosures Not Subject to Accounting.** TheBusiness Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of the Covered Entity’s Protected Health Information if the Covered Entity need not account for such disclosures under the HIPAA Rules.

**(iii) Disclosure Information.** With respect to any disclosure by the Business Associate of the Covered Entity’s Protected Health Information that is not excepted from disclosure accounting under the HIPAA Rules, the Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

**(A) Disclosure Information Generally.** Except for repetitive disclosures of the Covered Entity’s Protected Health Information as specified below, the Disclosure Information that the Business Associate must record for each accountable disclosure is (1) the disclosure date, (2) the name and (if known) address of the entity to which the Business Associate made the disclosure, (3) a brief description of the Covered Entity’s Protected Health Information disclosed, and (4) a brief statement of the purpose of the disclosure.

**(B) Disclosure Information for Repetitive Disclosures.** For repetitive disclosures of the Covered Entity’s Protected Health Information that the Business Associate makes for a single purpose to the same person or entity (including the Covered Entity), the Disclosure Information that the Business Associate must record is either the Disclosure Information specified above for each accountable disclosure, or (1) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (2) the frequency, periodicity, or number of the repetitive accountable disclosures; and (3) the date of the last of the repetitive accountable disclosures.

**(iv) Availability of Disclosure Information.** TheBusiness Associate will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates (3 years for disclosures related to an Electronic Health Record, starting with the date specified by HHS). The Business Associate will make the Disclosure Information available to the Covered Entity withinfifty (50) calendar days following the Covered Entity’s request for such Disclosure Information to comply with an individual’s request for disclosure accounting. Effective as of the date specified by HHS, with respect to disclosures related to an Electronic Health Record, the Business Associate shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

**(d) *Restriction Agreements and Confidential Communications.*** The Covered Entity shall notify the Business Associate of any limitations in the notice of privacy practices of the Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect the Business Associate’s use or disclosure of Protected Health Information. TheBusiness Associate will comply with any agreement that the Covered Entity makes that either (i) restricts use or disclosure of the Covered Entity’s Protected Health Information pursuant to 45 CFR §164.522(a), or (ii) requires confidential communication about the Covered Entity’s Protected Health Information pursuant to 45 CFR §164.522(b), provided that the Covered Entity notifies the Business Associate in writing of the restriction or confidential communication obligations that the Business Associate must follow. The Covered Entity will promptly notify the Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct the Business Associate whether any of the Covered Entity’s Protected Health Information will remain subject to the terms of the restriction agreement. Effective February 17, 2010 (or such other date specified as the effective date by HHS), the Business Associate will comply with any restriction request if: (i) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

**VII. Breaches and Security Incidents**

**(a) *Reporting.***

1. **Impermissible Use or Disclosure.** The Business Associate will report to Covered Entity any use or disclosure of Protected Health Information not permitted by this Agreement not more than fifty (50) calendar days after Business Associate becomes aware of such non-permitted use or disclosure.
2. **Privacy or Security Breach.** The Business Associate will report to the Covered Entity any use or disclosure of the Covere**d** Entity’s Protected Health Information not permitted by this Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information as required by 45 CFR 164.40 and any Security Incident of which it becomes aware. The Business Associate will make the report to the Covered Entity’s Privacy Official not more than fifty (50) calendar days after the Business Associate becomes aware of such non-permitted use or disclosure. If a delay is requested by a law-enforcement official in accordance with 45 CFR §164.412, the Business Associate may delay notifying the Covered Entity for the applicable time period. The Business Associate’s report will at least:

(A) Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of the Breach;

(B) Identify the Covered Entity’s Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual basis;

(C) Identify who made the non-permitted use or disclosure and who received the non-permitted use or disclosure;

(D) Identify what corrective or investigational action the Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

(E) Identify what steps the individuals who were subject to a Breach should take to protect themselves; and

(F) Provide such other information, including a written report and risk assessment under 45 CFR 164.402, as the Covered Entity may reasonably request.

**(ii) Security Incidents. T**he Business Associate will report to The Covered Entity any Security Incident of which the Business Associate becomes aware. The Business Associate will make this report \_once per month, except if any such Security Incident resulted in a disclosure not permitted by this Agreement or Breach of Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth above.

(b) **Mitigation**. The Business Associate shall mitigate, to the extent practicable, any harmful effect known to the Business Associate resulting from a use or disclosure in violation of this Agreement.

**VIII. Term and Termination**

**(a) *Term.*** The term of this Agreement shall be effective as of as of the date specified above, and shall terminate when all Protected Health Information provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

**(b) *Right to Terminate for Cause.*** TheCovered Entity may terminate this Agreement if it determines, in its sole discretion, that the Business Associate has breached a material provision of this Agreement, and upon written notice to the Business Associate of the breach, the Business Associate fails to cure the breach within thirty (30) calendar days after receipt of the notice. Any such termination will be effective immediately or at such other date specified in the Covered Entity’s notice of termination.

**(c) *Treatment of Protected Health Information on Termination.***

**(i) Return or Destruction of Covered Entity’s Protected Health Information as Feasible.**

Upon termination or other conclusion of this Agreement, the Business Associate will, if feasible, return to the Covered Entity or destroy all of the Covered Entity’s Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the Covered Entity’s Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of the Business Associate. Further, the Business Associate shall require any such Subcontractor or agent to certify to the Business Associate that it returned to the Business Associate (so that the Business Associate may return it to the Covered Entity) or destroyed all such information which could be returned or destroyed. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Agreement.

**(ii) Procedure When Return or Destruction Is Not Feasible.** TheBusiness Associate will identify any of the Covered Entity’s Protected Health Information, including any that the Business Associate has disclosed to subcontractors or agents as permitted under this Agreement, that cannot feasibly be returned to the Covered Entity or destroyed and explain why return or destruction is infeasible. The Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Agreement.

**(iii) Continuing Privacy and Security Obligation.** TheBusiness Associate’s obligation to protect the privacy and safeguard the security of the Covered Entity’s Protected Health Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

**IX. Miscellaneous Provisions**

**(a) *Definitions.*** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance.

**(b) *Inspection of Internal Practices, Books, and Records.*** TheBusiness Associate will make its internal practices, books, and records relating to its use and disclosure of the Covered Entity’s Protected Health Information available to the Covered Entity and to HHS to determine compliance with the HIPAA Rules.

**(c) *Amendment to Agreement.*** This Amendment may be amended only by a written instrument signed by the parties. In case of a change in applicable law, the parties agree to negotiate in good faith to adopt such amendments as are necessary to comply with the change in law..

**(d) *No Third-Party Beneficiaries.*** Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.

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

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

**(g)** ***Interpretation*.**Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply with the HIPAA Rules.

**(h)** ***Notices*.** All notices hereunder shall be in writing and delivered by hand, by certified mail, return receipt requested or by overnight delivery. Notices shall be directed to the parties at their respective addresses set forth in the first paragraph of this Business Associate Agreement or below their signature, as appropriate, or at such other addresses as the parties may from time to time designate in writing.

**(i) *Entire Agreement; Modification*.** This Business Associate Agreement represents the entire agreement between the Business Associate and the Covered Entity relating to the subject matter hereof. No provision of this Business Associate Agreement may be modified, except in writing, signed by the parties.

**(j)** ***Indemnification.*** Each Party agrees to indemnify, defend and hold harmless each other Party, its affiliates and each of their respective directors, officers, employees, agents or assigns from and against any and all actions, causes of actions, claims, suits and demands whatever, and from all damages, liabilities, costs, charges, debts and expenses whatever (including reasonable attorneys’ fees and expenses related to any litigation or other defense of any claims), which may be asserted or for which they may now or hereafter become subject arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the Party to the Agreement and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of any way connected with the Party’s performance.

**(k)** ***Assistance in Litigation or Administrative Proceedings*.** The Business Associate shall make itself, and any subcontractors, employees or agents assisting the Business Associate in the performance of its obligations under this Agreement, available to the Covered Entity, at no cost to the Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its directors, officers, or employees based upon a claimed violation of HIPAA, the HIPAA regulations, or other laws relating to security and privacy, except where the Business Associate or its subcontractors, employees, or agents are named as an adverse party.

**(l) *Binding Effect*.** This Business Associate Agreement shall be binding upon the parties hereto and their successors and assigns.

**(m)** **Governing Law, Jurisdiction, and Venue**. This Agreement shall be governed by the law of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, except to the extent preempted by federal law.

**(n) Severability**. The invalidity or unenforceability of any provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

**(o) Construction and Interpretation**. The section headings contained in this Agreement are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement. This Agreement has been negotiated by the parties at arm's-length and each of them has had an opportunity to modify the language of the Agreement. Accordingly, the Agreement shall be treated as having been drafted equally by the parties, and the language shall be construed as a whole and according to its fair meaning. Any presumption or principle that the language is to be construed against any party shall not apply. This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

**In Witness Whereof**, the parties hereto have caused this Agreement to be executed as of the date first above written.

**BUSINESS ASSOCIATE: COVERED ENTITY:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ HEALTH PLAN

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Notice of Privacy Practices**

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

This Notice of Privacy Practices describes the legal obligations of following plans of *[Insert Name of Employer*] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[Insert name of plans](the “Plans”) and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health information Technology for Economic and Clinical Health Act (“HITECH”). This Notice has been drafted in accordance with the HIPAA Privacy Rule, contained the in the Code of Federal Regulations at 45 CFR Parts 160 and 164. Terms not defined in this Notice have the same meaning as they have in the HIPAA Privacy Rule.

Among other things, this Notice describes how your protected health information may be used or disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law.

We are required to provide this Notice of Privacy Practices (the “Notice”) to you pursuant to HIPAA.

The HIPAA Privacy Rule protects only certain medical information known as “protected health information.” Generally, protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, or your employer on behalf of a group health plan that relates to:

(1) Your past, present or future physical or mental health or condition;

(2) The provision of health care to you; or

(3) The past, present or future payment for the provision of health care to you.

If you have any questions about this Notice or about our privacy practices, please contact *[insert name or title, and telephone number of person or office to contact].*

**Effective Date**

This Notice is effective *[insert date.* ***Note:*** *the effective date may not be earlier than the date on which the Notice is printed or otherwise published].*

**Our Responsibilities**

We are required by law to:

* Maintain the privacy of your protected health information;
* Inform you promptly if a breach occurs that may have compromised the privacy or security of your information;
* Provide you with certain rights with respect to your protected health information;
* Provide you with a copy of this Notice of our legal duties and privacy practices with respect to your protected health information;
* Follow the terms of the Notice that is currently in effect; and
* Not use or share your information other than as described here unless you tell us in writing that we can. If you tell us we can share information, you may change your mind at any time and advise us in writing of such change.

We reserve the right to change the terms of this Notice and to make new provisions regarding your protected health information that we maintain, as allowed or required by law. If we make any material change to this Notice, we will provide you with a copy of our revised Notice of Privacy Practices by *[describe how Plan will provide individuals with a revised notice—e.g., by mail to their last-known address on file].*

**How We May Use and Disclose Medical Your Protected Health Information**

Under the law, we may use or disclose your protected health information under certain circumstances without your permission. The following categories describe the different ways that we may use and disclose your protected health information. For each category of uses or disclosures we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

**For Treatment.**

We may use or disclose your protected health information to facilitate medical treatment or services by providers. We may disclose medical information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you. For example, we might disclose information about your prior prescriptions to a pharmacist to determine if prior prescriptions contra indicate a pending prescription. *[Use where health plan is involved in rendering medical services.]*

**For Payment.**

We may use or disclose your protected health information to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, we may tell your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. We may also share your protected health information with a utilization review or pre-certification service provider. Likewise, we may share your protected health information with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.

**For Health Care Operations.**

We may use and disclose your protected health information for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, we may use medical information in connection with conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss (or excess-loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud & abuse detection programs; business planning and development such as cost management; and business management and general Plan administrative activities. If use or disclosure of protected health information is made for underwriting purposes, any such protected health information that is genetic information of an individual is prohibited from being used or disclosed.

**To Business Associates.**

We may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain types of services. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your protected health information, but only after they agree in writing with us to implement appropriate safeguards regarding your protected health information. For example, we may disclose your protected health information to a Business Associate to administer claims or to provide support services, such as utilization management, pharmacy benefit management or subrogation, but only after the Business Associate enters into a Business Associate Agreement with us.

**As Required by Law.**

We will disclose your protected health information when required to do so by federal, state or local law, including with the Department of Health and Human Services if it wants to see that we are complying with federal privacy law. For example, we may disclose your protected health information when required by national security laws or public health disclosure laws.

**To Assist with Public Health and Safety Issues.**

We may use and disclose your protected health information when necessary to prevent a serious threat to your health and safety, or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, we may disclose your protected health information in a proceeding regarding the licensure of a physician.

**To Plan Sponsors.**

For the purpose of administering the plan, we may disclose to certain employees of the Employer protected health information. However, those employees will only use or disclose that information only as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your protected health information cannot be used for employment purposes without your specific authorization.

**Special Situations**

In addition to the above, the following categories describe other possible ways that we may use and disclose your protected health information. For each category of uses or disclosures, we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

**Organ and Tissue Donation.**

If you are an organ donor, we may release your protected health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

**Military and Veterans.**

If you are a member of the armed forces, we may release your protected health information as required by military command authorities. We may also release protected health information about foreign military personnel to the appropriate foreign military authority.

**Workers’ Compensation.**

We may release your protected health information for workers’ compensation or similar programs. These programs provide benefits for work-related injuries or illness.

**Public Health Risks.**

We may disclose your protected health information for public health actions. These actions generally include the following:

* To prevent or control disease, injury or disability;
* To report births and deaths;
* To report child abuse or neglect;
* To report reactions to medications or problems with products;
* To notify people of recalls of products they may be using;
* To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
* To notify the appropriate government authority if we believe that a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree, or when required or authorized by law.

**Health Oversight Activities.**

We may disclose your protected health information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

**Lawsuits and Disputes.**

If you are involved in a lawsuit or a dispute, we may disclose your protected health information in response to a court or administrative order. We may also disclose your protected health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

**Law Enforcement.**

We may disclose your protected health information if asked to do so by a law enforcement official:

* In response to a court order, subpoena, warrant, summons or similar process;
* To identify or locate a suspect, fugitive, material witness, or missing person;
* About the victim of a crime if, under certain limited circumstances, we are unable to obtain the victim’s agreement;
* About a death that we believe may be the result of criminal conduct;
* About criminal conduct; and
* In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

**Coroners, Medical Examiners and Funeral Directors.**

We may release protected health information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients to funeral directors as necessary to carry out their duties.

**National Security and Intelligence Activities.**

We may release your protected health information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

**Inmates.**

If you are an inmate of a correctional institution or are under the custody of a law enforcement official, we may disclose your protected health information to the correctional institution or law enforcement official if necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

**Research.**

We may disclose your protected health information to researchers when:

1. The individual identifiers have been removed; or
2. When an institutional review board or privacy board (a) has reviewed the research proposal; and (b) established protocols to ensure the privacy of the requested information, and approves the research.

**Required Disclosures**

The following is a description of disclosures of your protected health information we are required to make.

**Government Audits.**

We are required to disclose your protected health information to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA privacy rule.

**Disclosures to You.**

When you request, we are required to disclose to you the portion of your protected health information that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. We are also required, when requested, to provide you with an accounting of most disclosures of your protected health information where the disclosure was for reasons other than for payment, treatment or health care operations, and where the protected health information not disclosed pursuant to your individual authorization.

**Your Choices**

**For certain health information, you can tell us your choices about what we share.** If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

* Share information with your family, close friends, or others involved in payment for your care
* Share information in a disaster relief situation

*If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*

**Personal Representatives.**

We will disclose your protected health information to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc., so long as you provide us with a written notice/authorization and any supporting documents (i.e., power of attorney). Note: Under the HIPAA privacy rule, we do not have to disclose information to a personal representative if we have a reasonable belief that:

1. You have been, or may be, subjected to domestic violence, abuse or neglect by such person;
2. Treating such person as your personal representative could endanger you; or
3. In the exercise of professional judgment, it is not in your best interest to treat the person as your personal representative.

**Fundraising and Marketing**

Prior to disclosing your protected health information in the case of any fundraising efforts, you will be notified prior to receiving such fundraising communications. Such communication will provide you with the option of opting-out of receiving such communications. Additionally, uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI will require authorization.

**Spouses and Other Family Members.**

With only limited exceptions, we will send all mail to the employee. This includes mail relating to the employee's spouse and other family members who are covered under the Plans, and includes mail with information on the use of Plan benefits by the employee's spouse and other family members and information on the denial of any Plan benefits to the employee's spouse and other family members. If a person covered under the Plan has requested Restrictions or Confidential Communications (see below under “Your Rights”), and if we have agreed to the request, we will send mail as provided by the request for Restrictions or Confidential Communications.

**Authorizations.**

Other uses or disclosures of your protected health information not described above will only be made with your written authorization. Most uses and disclosures of psychotherapy notes (when appropriate) will require your authorization.

You may revoke written authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation.

**Your Rights**

You have the following rights with respect to your protected health information:

**Right to Access.**

You have the right to inspect and copy certain protected health information that may be used to make decisions about your health care benefits. To inspect and copy your protected health information, you must submit your request in writing to *[insert name of Employer Contact]*. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing or other supplies associated with your request.

Additionally, you have the right to request electronic copies of certain protected health information in a designated record set. We will provide such information in the electronic form and format requested by you, provided it is readily producible. If the requested form and format are not readily producible, we will provide the information in a readable electronic form and format that is mutually agreed upon with you. If you request a copy of the electronic information, we may charge a reasonable fee for the labor costs and supplies involved in creating the information.

We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a written request to [*insert name of Employer Contact*].

**Right to Amend.**

If you feel that the protected health information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, your request must be made in writing and submitted to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name of Employer Contact*]. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

* Is not part of the medical information kept by or for the Plan;
* Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
* Is not part of the information that you would be permitted to inspect and copy; or
* Is already accurate and complete.

If we deny your request, we will notify you in writing within 60 days with an explanation as to why the request was denied. You then have the right to file a statement of disagreement with us and any future disclosures of the disputed information will include your statement.

**Right to an Accounting of Disclosures.**

You have the right to request an “accounting” of certain disclosures of your protected health information. The accounting will not include (1) disclosures for purposes of treatment, payment, or health care operations; (2) disclosures made to you; (3) disclosures made pursuant to your authorization; (4) disclosures made to friends or family in your presence or because of an emergency; (5) disclosures for national security purposes; and (6) disclosures incidental to otherwise permissible disclosures.

To request this list or accounting of disclosures, you must submit your request in writing to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name and address of Employer Contact]*. Your request must state a time period of not longer than six years prior to the date you ask for the accounting.

Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be provided free of charge. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

**Right to Request Restrictions.**

You have the right to request a restriction or limitation on your protected health information that we use or disclose for treatment, payment or health care operations. You also have the right to request a limit on your protected health information that we disclose to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had.

If you request a restriction, it is your responsibility to notify any other entity that may be impacted by the requested restriction.

Except as provided in the next paragraph, we are not required to agree to your request. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you.

Effective February 17, 2010 (or such other date specified as the effective date under applicable law), we will comply with any restriction request if: (1) except as otherwise required by law, the disclosure is to the health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

To request restrictions, you must make your request in writing to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name and address of Employer Contact]*. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure, or both; and (3) to whom you want the limits to apply—for example, disclosures to your spouse.

**Right to Request Confidential Communications.**

You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

To request confidential communications, you must make your request in writing to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name and address of Employer Contact]*. We will not ask you the reason for your request. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your protected information could endanger you.

**Right to be Notified of a Breach.**

You have the right to receive to be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information. Notice of a breach will be provided to you within 60 days of the breach being identified.

**Right to a Paper Copy of This Notice.**

You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice.

You may obtain a copy of this notice at our website, www.\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert Employer website address].*

To obtain a paper copy of this notice, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name and address of Contact*].

**Right to Choose Someone to Act for You.**

You have the right to appoint a personal representative to act on your behalf with respect to your protected health information, such as if you have given someone medical power of attorney or if someone is your legal guardian.

To appoint a personal representative to act on your behalf, you must make your request in writing to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [*insert name and address of Employer Contact]*. Your request must specify who the individual is that you are appointing, that individual’s contact information, and in which matters the appointed individual may act on your behalf.

**Right to File Complaints.**

If you believe that your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights. To file a complaint with the Plan, contact \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *[insert the name, title, and phone number of the contact person or office responsible for handling complaints—this should be the same person or department listed on the first page as the contact for more information about this notice]*. All complaints must be submitted in writing. A complaint to the Office of Civil Rights should be sent to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *[insert appropriate OCR contact address for region]* or by visiting [www.hhs.gov/ocr/privacy/hipaa/complaints/](http://www.hhs.gov/ocr/privacy/hipaa/complaints/).

You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office of Civil Right

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**(Name of Plan)**

**AUTHORIZATION FOR RELEASE OF INFORMATION**

**I. Information About the Use or Disclosure**

**I hereby authorize the use or disclosure of my individually identifiable health information as described below.** I understand that this authorization is voluntary and that I may refuse to sign this authorization, and that I may revoke it at any time by submitting my revocation in writing to the entity providing the information.

Individual’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Persons/organizations authorized to provide the information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Persons/organizations authorized to receive the information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Specific description of information to be used or disclosed (including date(s)): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Specific purpose of the disclosure: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will the health plan or health care provider requesting the authorization receive financial or in-kind compensation in exchange for using or disclosing the health information described above?

No \_\_\_ Yes \_\_\_ (describe) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This authorization will expire \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (indicate date, or an event relating to you personally or to the purpose of the authorization).

**II. Important Information About Your Rights**

I have read and understood the following statements about my rights:

* I may revoke this authorization at any time prior to its expiration date by notifying the providing organization, in writing, but the revocation will not have any effect on any actions that the entity took before it received the revocation.
* I may see and copy the information described on this form if I ask for it.
* I am not required to sign this form to receive my health care benefits (enrollment, treatment, or payment).
* The information that is used or disclosed pursuant to this authorization may be redisclosed by the receiving entity. I have the right to seek assurances from the above-named persons/organizations authorized to receive the information that they will not redisclose the information to any other party without my further authorization.

**III. Signature of Individual’s or Individual’s Representative**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of individual or individual’s representative Date

(Form MUST be completed before signing.)

Printed name of the individual’s representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Relationship to the individual, including authority for status as representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**HIPAA SECURITY STANDARDS CHECKLIST**

**INTRODUCTION**

There are two different types of security standards; “Required” compliance standards and “Addressable” compliance standards. Required standards are designated with a (R) on the following checklist and Addressable standards are designated with an (A) on the checklist. All covered entities must comply with the Required standards. With respect to the Addressable standards, every covered entity must: (1) assess whether the standard is reasonable and appropriate in its particular environment, when analyzed with the likely contributions protecting the entity’s electronic protected information; and (2) implement the standard if it is reasonable and appropriate; or (a) document why it would not be reasonable and appropriate to implement the standard; and (b) implement an equivalent alternative measure if one is reasonable and appropriate.

**ADMINISTRATIVE SAFEGUARDS** (§164.308(a))

□ **SECURITY MANAGEMENT PROCESS**

□ Risk Analysis (R). Conduct an *accurate and thorough* assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (“e-PHI”) held by the covered entity. §164.308(a)(1)(ii)(A).

□ Risk Management (R). Implement security measures that reduce risk and vulnerabilities to a “reasonable and appropriate level.” §164.308(a)(1)(ii)(B).

□ Sanction Policy (R). “Apply appropriate sanctions” against workforce members who fail to comply with its security policies and procedures. §164.308(a)(1)(ii)(C).

□ Information System Activity Review (R). Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incidence tracking reports. §164.308(a)(1)(ii)(D).

□ **ASSIGN SECURITY OFFICIAL (R)**

Identify a “security official” who is responsible for the development and implementation of necessary security policies and procedures. §164.308(a)(2).

□ **WORKFORCE SECURITY**

□ Authorization/Supervision Procedures (A) Implement procedures to provide for the authorization and supervision of workforce members who work with e-PHI information or who work in locations where it might be accessed. §164.308(a)(3)(ii)(A).

□ Workforce Clearance Procedures (A). Implement procedures to determine whether the access of a workforce member to electronic health information is appropriate. §164.308(a)(3)(ii)(B).

□ Access Termination Procedures (A). Implement procedures to terminate an individual’s access to electronic protected health information when necessary or appropriate. §164.308(a)(3)(ii)(C).

□ **INFORMATION ACCESS MANAGEMENT**

□ Isolating Health Care Clearinghouse Functions (R). If a health care clearinghouse is part of a larger organization, that clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. §164.308(a)(4)(ii)(A).

□ Access Authorization (A). Implement policies and procedures for granting access to e-PHI (e.g., through access to a workstation or other source). §164.308(a)(4)(ii)(B).

□ Access Establishment and Modification (A). Implement policies and procedures that establish, document, review and modify a user’s right to access a workstation or other similar location. §164.308(a)(4)(ii)(C).

□ **SECURITY AWARENESS AND TRAINING**

□ Security Reminders (A). Provide periodic security updates to all members of its workforce. §164.308(a)(5)(ii)(A).

□ Software Protection (A). Implement procedures to detect and guard against viruses and other malicious software. §164.308(a)(5)(ii)(B).

□ Log-In Monitoring (A). Implement procedures to monitor attempts to log-in to any system that holds electronic health information and to report discrepancies in attempted log-ins. §164.308(a)(5)(ii)(C).

□ Password Management (A). Implement procedures to create, change and safeguard passwords. § 164.308(a)(5)(ii)(D).

□ **SECURITY INCIDENT PROCEDURES**

□ Identify and Respond to Security Incidents (R). Implement policies and procedures to identify and respond to suspected or known security incidents and document security incidents and their outcomes. §164.308(a)(6)(ii).

□ Mitigate Known Security Incidents (R). Implement policies and procedures to mitigate, to the extent practicable, harmful effects of any security breach or incident that is known to the covered entity. §164.308(a)(6)(ii).

□ Document Security Incidents (R). Implement policies and procedures that will document each security incident and its outcome. §164.308(a)(6)(ii).

□ **CONTINGENCY PLAN**

□ Data Backup Plan (R). Implement policies and procedures to create and maintain retrievable “exact” copies of e-PHI. §164.308(a)(7)(ii)(A).

□ Disaster Recovery Plan (R). Establish and implement any necessary procedures to restore lost data. §164.308(a)(7)(ii)(B).

□ Emergency Operation Plan (R). Establish and implement any necessary procedures to enable the continuation of critical business processes needed to protect the security of e-PHI while operating in an emergency mode. §164.308(a)(7)(ii)(C).

□ Testing and Revision Procedures (A). Implement procedures that allow for the periodic testing and revision of contingency plans. §164.308(a)(7)(ii)(D).

□ Applications and Data Criticality Analysis (A). Assess the relative importance of specific applications and data in support of other contingency plan components. §164.308(a)(7)(ii)(E).

□ **EVALUATION (R).**

Perform technical and non-technical evaluations of the entity’s security policies and procedures and in response to environmental or operational changes affecting the security of e-PHI that establishes the extent to which an entity's security policies and procedures meet the requirements of the regulations §164.308(a)(7).

**BUSINESS ASSOCIATE CONTRACTS AND OTHER AGREEMENTS**

**(§§ 164.308(b) and 164.314)**

□ **BUSINESS ASSOCIATE CONTRACTS (R).**

A covered entity may generally permit a business associate to create, receive, maintain or transmit e-PHI on its behalf only if it enters into an appropriate business associate contract or arrangement with that business associate. The business associate contract or arrangement must provide that the business associate will:

□ Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the e-PHI that it creates, receives, maintains or transmits on behalf of the covered entity. §164.314(a)(2)(i)(A).

□ Ensure that any agent, including a sub-contractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect the e-PHI. §164.314(a)(2)(i)(B).

□ Report to the covered entity any security incidents of which it becomes aware. § 164.314(a)(2)(i)(C).

□ Authorize the termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract, unless this requirement is inconsistent with the statutory obligations of the covered entity or the business associate. §164.314(a)(2)(i)(D).

□ Group HealthPlans **(R).**

In most instances, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard e-PHI created, received, maintained or transmitted to or by the plan sponsor. Accordingly, the plan documents of the group’s health plan must be amended to incorporate the following provisions to require the plan sponsor to:

□ Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of e-PHI that the plan sponsor creates, receives, maintains or transmits on behalf of the group health plan. §164.314(b)(2)(i).

□ Ensure that there is an adequate separation (or fire wall) between the information that is received from the group health plan and other employment information and decisions and this separation is supported by reasonable and appropriate security measures. §164.314(b)(2)(ii).

□ Ensure that any agent, including a sub-contractor, to whom the plan sponsor provides this information, agrees to implement reasonable and appropriate security measures to protect the information. §164.314(b)(2)(iii).

□ Report to the welfare benefit plan any security incident of which the plan sponsor becomes aware of. §164.314(b)(2)(iv).

**PHYSICAL SAFEGUARDS (§164.310)**

□ **FACILITY ACCESS CONTROLS**

□ Contingency Operations (A). Establish and implement any necessary procedures to allow access to the facility to support the restoration of lost data under a disaster recovery plan and an emergency mode operations plan. §164.310(a)(2)(i).

□ Facility Security Plan (A). Implement policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering and theft. §164.310(a)(2)(ii).

□ Access Control and Validation Procedures (A). Implement procedures to control and validate a person’s access to facilities based upon their role or function (including visitor control) and to control access to software programs for testing and revision. §164.310(a)(2)(iii).

□ Maintenance Records (A). Implement policies and procedures to document any repairs or modifications to the physical components of a facility which are related to its security (hardware, walls, doors, and locks). §164.310(a)(2)(iv).

□ **WORKSTATION USE (R).**

Implement policies and procedures specific to the functions that are to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of the specific workstation or class of workstation that can access e-PHI. §164.310(b).

□ **WORKSTATION SECURITY (R).**

Implement physical safeguards restricting unauthorized access to authorized users-only information for all workstations that have the ability to access e-PHI. §164.310(c).

□ **DEVICE AND MEDIA CONTROLS**

□ Disposal (R). Implement policies and procedures to address the final disposition of e-PHI and/or the hardware or electronic media on which e-PHI has been stored. §164.310(d)(2)(i).

□ Media Re-Use (R). Implement procedures for removal of e-PHI from electronic media before the media is made available for re-use. §164.310(d)(2)(ii).

□ Accountability (A). Maintain a record of the movements of hardware and electronic media and any person responsible for such movements. §164.310(d)(2)(iii).

□ Data Backup and Storage (A). Create a retrievable, exact copy of e-PHI when needed, before movement or transfer of hardware or other electronic media. §164.310(d)(2)(iv).

**TECHNICAL SAFEGUARDS (§164.312)**

□ **ACCESS CONTROL**

□ Unique User Identification (R). Implement policies and procedures that assign a unique name and/or user number to identify and track user identity. §164.312(a)(2)(i).

□ Emergency Access Procedure (R). Establish and implement necessary procedures to obtain necessary e-PHI in an emergency. §164.312(a)(2)(ii).

□ Automatic Log-Off (A). Implement electronic procedures that terminate an electronic session after a pre-determined period of inactivity. §164.312(a)(2)(iii).

□ Encryption and Decryption (A). Implement a mechanism to encrypt and decrypt e-PHI. §164.312(a)(2)(iv).

□ **AUDIT CONTROLS (R).**

Implement hardware, software, and/or procedural mechanisms that record and examine activity on information systems that contain or use e-PHI. §164.312(b).

□ **INTEGRITY (A).**

Implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner. §164.312(c)(2).

□ **USER AUTHENTICATION (R).**

Implement procedures to verify that a person or entity seeking to access e-PHI is the person or entity claimed. §164.312(d).

□ **TRANSMISSION SECURITY**

□ Integrity Controls (A). Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until the e-PHI is disposed of. §164.312(e)(2)(i).

□ Encryption (A). Implement a mechanism to encrypt e-PHI whenever it is deemed appropriate. §164.312(e)(2)(ii).

**POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS (§164.316)**

□ **POLICIES AND PROCEDURES (R).**

Implement reasonable and appropriate policies and procedures to comply with the security standards. Covered entities may change their policies and procedures at any time, provided that the changes are documented and implemented in accordance with the security regulations. §164.316(a).

□ **DOCUMENTATION.**

□ Document Policies and Procedures (R). Maintain written (which may be electronic) policies and procedures that are implemented to comply with the security regulations. §164.316(b)(1)(i).

□ Document Action, Activities and Assessments (R). Maintain a written (which may be electronic) record of any action, activity or assessment required under the security regulations. §164.316(b)(1)(ii).

□ Time Limits (R). Retain all documentation required for six years from the date of its creation or the date when it was last in effect, whichever is later. §164.316(b)(2)(i).

□ Availability (R). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. §164.316(b)(2)(ii).

□ Updates (R). Review documentation periodically and update that information as necessary to respond to environmental or operational changes that affect the security of e-PHI. §164.316(b)(2)(iii).

This checklist was completed by the individual indicated below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Individual Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

**PLAN SPONSOR CERTIFICATION**

*[Insert Name of Employer]* (the “Plan Sponsor”), the sponsor of the *[Insert Name of Plan]* (the “Plan”), a “group health plan” as defined 45 CFR § 164.160, hereby certifies that the Plan documents that govern the Plan have been amended to incorporate the following provisions and the Plan Sponsor shall:

* not use or further disclose the PHI other than as permitted or required by the Plan or as required by law;
* ensure that any agent, including a subcontractor, to whom it provides PHI received from the Plan agrees to and complies with the same restrictions and conditions that apply to the Plan Sponsor with respect to PHI;
* not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor;
* report to the Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
* make available PHI to comply with HIPAA’s right to access in accordance with 45 CFR § 164.524;
* make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR § 164.526;
* make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528;
* make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of Health and Human Services for purposes of determining compliance by the Plan with HIPAA’s privacy requirements;
* if feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
* ensure that the adequate separation between Plan and Plan Sponsor (i.e., the “firewall”), required in 45 CFR § 504(f)(2)(iii), is satisfied.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plan Sponsor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**HIPAA Privacy Compliance Checklist**

| **Task** | **Tasks**  **Assigned to** | **Status/Work**  **Performed** |
| --- | --- | --- |
| **Obtain Education on HIPAA Privacy Requirements** | | |
| 1. HIPAA EDI requirements. |  |  |
| 2. HIPAA privacy requirements. |  |  |
| **Organize the HIPAA Privacy Team and Create a Game Plan** | | |
| 1. Obtain requisite board and management approval to develop HIPAA implementation team and plan. |  |  |
| 2. Establish a privacy budget. |  |  |
| 3. Assemble the HIPAA privacy team.   * identify all departments that should be represented (e.g., HR, benefits, accounting, information systems, legal, etc.) * identify individuals from each department to be part of privacy team. |  |  |
| 4. Appoint a privacy officer. |  |  |
| 5. Establish internal timeline and meeting schedule |  |  |
| **Assess the Way Health Information Is Currently Handled Within the Employer** | | |
| 1. Identify health plans subject to HIPAA and individuals with access to health information—   * identify health plans subject to HIPAA * identify internal personnel with access to health information * describe known uses for health information * list outside entities/vendors with which health information is shared * list outside entities/vendors that provide health information |  |  |
| 2. Identify non-health plans and programs with access to health information—   * identify non-health plans/programs subject to HIPAA * identify internal personnel with access to health information * describe known uses for health information * list outside entities/vendors with which health information is shared * list outside entities/vendors that provide health information |  |  |
| 3. Identify additional individuals with access to health information e-mail/intranet survey. |  |  |
| 4. Identify specific health information exchanges engaged in by personnel identified in Steps 1-3—   * identify specific health information uses and disclosures * identify purpose for which health information is currently used and disclosed * identify source of health information * identify outside entities with which health information is shared (and purpose of sharing information) * determine whether release/authorizations are currently used * determine privacy policies, procedures and safeguards currently in place |  |  |
| **Evaluate the Employer’s Need for Protected Health Information and Desired Approach (“Hands Off” or “Involved”)** | | |
| In complying with the HIPAA privacy rules, the regulations allow plan sponsor to choose between the “Hands-Off PHI” Approach and the “Hands-On” Approach   * “Hands-Off PHI” Approach: Group health plans that provide health benefits only through an insurance contract (fully-insured plans), and that do n*ot* create, maintain, or receive PHI, can largely avoid the burdensome privacy requirements * “Hands-On” Approach: Group health plans that either are self-insured or are fully insured and create, maintain, or receive PHI (in addition to summary health information and enrollment information) are subject to all of HIPAA privacy requirements |  |  |
| Based on information obtained from the inquiries outlined above, the Employer must decide, with regard to *each* of its plans, whether it will adopt the “Hands-On” Approach or the “Hands-Off” PHI Approach. |  |  |
| In choosing between the “Hands-Off PHI” Approach and the “Hands-On” Approach, the Employer must evaluate the benefits it offers, as well as its current level of involvement in administering health plans. |  |  |
| 1. List the various benefits offered (i.e., medical, dental, health FSA, EAP, vision, etc.). |  |  |
| 2. Identify whether each of the benefits is fully insured or self-insured. |  |  |
| 3. Identify the type of PHI that is involved with each benefit. |  |  |
| 4. Identify the purposes for which the PHI is currently being used within the Employer. These purposes should then be divided into three categories:   * uses permitted by the privacy rules without an authorization * non-permitted uses that are deemed vital, and for which an employee authorization should thus be obtained * non-permitted uses that are not vital and should thus be discontinued |  |  |
| 5. Evaluate whether other uses are necessary and permitted.   * determine whether such uses are permissible under the privacy rules * if not, evaluate whether the uses are vital enough to seek an employee authorization so that the uses are permitted under the rules |  |  |
| 6. Determine whether any safeguards are already in place to protect the PHI.   * compare these safeguards to those that are required by HIPAA (discussed below) determine what changes will need to be made |  |  |
| 7. For fully-insured benefits, determine the extent to which the Employer desires to have PHI access that extends beyond the following t two scenarios:   * obtaining from the group health plan or its health insurance issuer (upon request) “summary health information” for the limited purposes of (a) obtaining premium bids for providing health insurance coverage under the group health plan; or (b) modifying, amending or terminating the group health plan * obtaining information relating to enrollment and disenrollment under the group health plan. The Employer can choose the “Hands-Off PHI” approach if it is willing to limit its access to PHI these two scenarios. |  |  |
| **“Hands-On” Approach** | | |
| Health plans are subject to the following HIPAA administrative requirements if the Employer adopts the “Hands-On” approach. Health plans (acting through the privacy officer) should ensure that compliance with the HIPAA’s privacy rule is well documented. |  |  |
| 1. Administrative requirements   * appoint a privacy officer; * establish policies and procedures for the use and disclosure of PHI; * establish a complaint office; * train employees regarding privacy rules; * adopt a sanctions policy for employees that violate the HIPAA privacy rule; * adopt procedures prohibiting retaliation against individuals who exercise HIPAA rights and to avoid a waiver of those rights; and * establish physical, technical and administrative safeguards to protect PHI |  |  |
| 2. Prepare and distribute a Notice of Privacy Practices   * a description of uses and disclosures of PHI, * right to inspect and obtain a copy of PHI; * right to have the Plan amend PHI records; * right to request restrictions on certain disclosures of PHI and to request confidential communications of PHI; and * right to receive an accounting of disclosures of PHI made within past six years |  |  |
| 3. Design and implement internal procedures to permit individuals to exercise their HIPAA rights   * provide notice of privacy practices; * provide notice of right to inspect and obtain a copy of PHI, request amendment of PHI, request restrictions on certain uses and disclosures of PHI, request and received(if the request is reasonable) confidential communications of PHI by alternative means or at alternative locations and obtain an accounting of disclosures of PHI; and * explain where and how individual can file a HIPAA privacy complaint |  |  |
| It is important to remember that even after complying with these administrative requirements, the Employer can use PHI *only for limited purposes—* namely, for “plan administration functions” that are performed on behalf of the group health plan and that are specified in the plan document. Moreover, only the “minimum necessary” PHI can be disclosed to accomplish the function. Moreover, the privacy officer should ensure that the policies and procedures (and related documents) are reviewed and updated periodically to reflect changes in circumstances (including operational changes, structural changes, and personnel changes). |  |  |
| **Amend the Plan Document** | | |
| In order for a plan to disclose PHI to the Employer’s benefits personnel, the plan document must be amended to:   * describe the permitted and required uses and disclosures of PHI by the plan; * specify that disclosure is permitted only upon receipt of written certification that the plan documents have been amended; and * provide adequate firewalls   Each of these is discussed in more detail below. |  |  |
| 1. Describe the permitted and required uses and disclosures. The plan document must be amended to establish the permitted and required uses and disclosures of PHI. This must be addressed in the plan’s Notice of Privacy Practices. |  |  |
| 2. Include written certification that plan documents have been amended. The plan document must be amended to provide that the plan may disclose PHI to the Employer *only* if the Employer certifies that the plan documents have been amended to incorporate the following provisions and that the Employer agrees 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 health plan agree to and comply with the same restrictions and conditions that apply to the Employer; * not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan; * report to the health plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures; * make PHI available to plan participants, consider their amendments, and, upon request, provide them with an accounting of PHI disclosures; * make its internal practices and records relating to the use and disclosure of PHI received from the health plan available to HHS upon request; and * if feasible, return or destroy all PHI received from the health plan that the Employer maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made;( except that if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible). |  |  |
| 3. Erect firewalls. In order to ensure that “adequate separation” exists between the group health plan and the Employer, the plan must be amended to:   * describe the employees (or class of employees) who may be given access to PHI; * restrict access to and use by such employees to *plan administration functions* that the Employer performs for the health plan; and * provide a procedure for resolving any issues of non-compliance |  |  |
| **Erect Firewalls** | | |
| Covered entities are required to erect “firewalls” to prevent PHI from being used impermissibly. |  |  |
| 1. Evaluate the roles of all employees to determine which employees are involved in the administration of its benefit plans. |  |  |
| 2. Implement a procedure to ensure that only these designated employees have access to PHI, and even then, that they have access only to the PHI necessary to perform their duties for the plan. |  |  |
| 3. Implement a mechanism for ensuring that these employees do not use or disclose PHI in a way prohibited by the privacy regulations.   * provide educational training for employees concerning the HIPAA privacy rules, the statutory penalties associated with violation of the rules, and the Employer’s internal policies for dealing with such violations |  |  |
| **Develop Approach to Comply with Breach Notification Requirements** | | |
| An action plan is required to ensure compliance with notification requirements in instances where there is a breach of unsecured PHI. |  |  |
| 1. Establish processes for identifying and responding to breaches including mitigation of “compromises” the security or privacy of PHI. |  |  |
| 2. Establish breach notification procedures (to individuals, HHS, and in certain instances, to the media). |  |  |
| 3. Amend business associate contracts. |  |  |
| 4. Undertake workforce training. |  |  |
| 5. Comply with additional administrative requirements (e.g., revisions to policies and procedures, complaint process). |  |  |
| **Address Relationships With Outside Third Parties (Vendors, TPAs, etc.)** | | |
| The privacy regulations require that certain restrictions be placed on health information that flows from the Employer to third parties known as “business associates.” |  |  |
| 1, Identify which third parties constitute “business associates.” HIPAA provides that a “business associate” is a person who, on behalf of a covered entity (i.e., a health care provider, health plan, or health care clearinghouse)—  • performs or assists in performing a function or activity involving the use or disclosure of individually identifiable health information or involving any other function or activity regulated by HIPAA's administrative simplification rules; or  • provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, health information services, e-prescribing gateways, data transmission services, and subcontractors, of a covered entity. where the performance of such services involves providing such service provider with individually identifiable health information. |  |  |
| 2. Ensure that each business associate contract:   * describes the permitted and required uses and disclosures by the business associate, which may not exceed that which is allowed for the plan; * prohibits the business associate from disclosing the information further; * requires the business associate to implement safeguards to prevent the improper use and disclosure of information; * requires the business associate to report to the plan any improper use or disclosure of PHI; * imposes the same requirements on all of the business associate’s subcontractors; * requires the business associate to make available PHI in compliance with individuals’ rights to access, amend, and receive an accounting related to such PHI; * requires the business associate to make its internal books and records available to HHS for purposes of determining the covered entity’s compliance with HIPAA; * describes the steps the business associate is required to take with respect to breach notification requirements and mitigation of breaches; * requires the business associate to return or destroy PHI, if feasible, upon termination of the relationship; and authorizes the plan to terminate the contract if the business associate has violated a material term of the contract; * authorizes the plan to terminate the contract if the business associate has violated a material term of the contract |  |  |
| 3. Consider contractual provisions to address breaches ofe breaches the contract. The provisions could include a a unilateral right to terminate the contract upon a material breach of HIPAA obligations, as well as indemnity to the plan (and the Employer) for any damages that the plan (or the Company) may incur by reason of the business associate’s breach |  |  |
| 4. Ensure that *all* business associates properly sign the contract and educate the business associates regarding their responsibilities and obligations under the contract. |  |  |
| 5. Implement a program to address the plan’s obligations in the event a business associate breaches the contract.   * if the plan obtains knowledge of a pattern or practice by a business associate that violates the business associate contract, the plan is required to take reasonable steps to cure the breach or end the violation * if the reasonable steps are unsuccessful, the plan must terminate the business associate contract, or (if not feasible) report the business associate to HHS |  |  |
| **Evaluate Potential Impact of Privacy Regulations on Non-Health-Plan Operations** | | |
| Although the HIPAA privacy regulations are targeted at health plans, they will have some impact on non-health-plan operations (workers’ compensation, disability, work return, etc.) that rely on access to individual health information. It is therefore important that the Employer consider how its non health-plan operations may be affected by the privacy rules. Some areas to consider are set forth below. The Employer should evaluate all of its non-health plan operations to see if there are additional areas. |  |  |
| **Formalize Privacy Policy to Reflect Approach Taken and Specific Organizational Requirements** | | |
| 1. *Drug testing policies.* Medical providers generally will not perform drug tests without authorization by the employee. The regulations do not prohibit a plan from requiring an employee to provide such authorization as a prerequisite to his or her employment (but other federal laws, such as ADA, should be reviewed). |  |  |
| 2. *Disability, FMLA, life insurance underwriting and administration.* An employee’s authorization generally is required before the Employer can use PHI for non-health-plan purposes such as disability, FMLA, life insurance underwriting, etc. |  |  |
| 3. Other Current Uses of PHI |  |  |

**AMENDMENT TO THE [Insert Name of Plan]**

**(As Amended and Restated Effective \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)**

**WHEREAS**, [*Insert Name of Employer*] (the “Employer”) deems it desirable to make changes to the *[Insert Name of Plan*] (the “Plan) to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996; and

**WHEREAS**, under the Plan, the Employer has the authority to amend the Plan and the undersigned has authority through resolutions adopted by the Board of Directors to execute this amendment on behalf of Employer.

**IT IS THEREFORE AGREED**, that the Plan is hereby amended effective as of April 14, 2004, unless otherwise specified as follows:

**ARTICLE \_\_\_ - PROTECTED HEALTH INFORMATION**

**\_.01 Permitted Disclosure of Enrollment/Disenrollment Information**

The Plan may disclose to the Employer information on whether the individual is participating in the Plan, or is enrolled in or has disenrolled.

**\_.02 Permitted Uses and Disclosure of Summary Health Information**

The Plan may disclose Summary Health Information to the Employer, provided the Employer requests the Summary Health Information for the purpose of (a) obtaining premium bids from health plans for providing health insurance coverage under the Plan; or (b) modifying, amending, or terminating the Plan.

“Summary Health Information” means information that (a) summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the Employer had provided health benefits under the Plan; and (b) from which the information described at 42 CFR § 164.514(b)(2)(i) has been deleted, except that the geographic information described in 42 CFR § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five-digit zip code.

**\_.03 Permitted and Required Uses and Disclosure of Protected Health Information for Plan Administrative Purposes**

Unless otherwise permitted by law, and subject to the conditions of disclosure described in Section \_.04 and obtaining written certification pursuant to Section \_.06, the Plan (or an Insurer on behalf of the Plan) may disclose PHI to the Employer, provided the Employer uses or discloses such PHI only for Plan administration purposes. “Plan administration purposes” means administration functions performed by the Employer on behalf of the Plan, such as quality assurance, claims processing, auditing, and monitoring. Plan administration functions do not include functions performed by the Employer in connection with any other benefit or benefit plan of the Employer, and they do not include any employment related functions.

Notwithstanding the provisions of this Plan to the contrary, in no event shall the Employer be permitted to use or disclose PHI in a manner that is inconsistent with 45 CFR § 164.504(f).

**\_.04 Conditions of Disclosure for Plan Administration Purposes**

The Employer agrees that with respect to any PHI (other than

Enrollment/Disenrollment information and Summary Health Information, which are not subject to these restrictions) disclosed to it by the Plan (or an Insurer on behalf of the Plan) the Employer shall:

A. Not use or further disclose the PHI other than as permitted or required by the Plan or as required by law.

B. Ensure that any agent, including a subcontractor, to whom it provides PHI received from the Plan agrees to and complies with the same restrictions and conditions that apply to the Employer with respect to PHI.

C. Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Employer.

D. Report to the Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware.

E. Make available PHI to comply with HIPAA’s right to access in accordance with 45 CFR § 164.524.

F. Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR § 164.526.

G. Make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528.

H. Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of Health and Human Services for purposes of determining compliance by the Plan with HIPAA’s privacy requirements.

I. If feasible, return or destroy all PHI received from the Plan that the Employer still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

J. Ensure that the adequate separation between the Plan and the Employer (i.e., the “firewall”), required in 45 CFR § 504(f)(2)(iii), is satisfied.

**\_.05 Adequate Separation Between Plan and the Employer**

The Employer shall allow those classes of employees or other persons in the Employer’s control designated by the Employer to be given access to PHI. No other persons shall have access to PHI. These specified employees (or classes of employees) shall only have access to and use PHI to the extent necessary to perform the plan administration functions that the Employer performs for the Plan. In the event that any of these specified employees do not comply with the provisions of this Section, that employee shall be subject to disciplinary action by the Employer for non-compliance pursuant to the Employer’s employee discipline and termination procedures.

**\_.06 Certification of the Employer**

The Plan shall disclose PHI to the Employer only upon the receipt of a certification by the Employer that the Plan has been amended to incorporate the provisions of 45 CFR §164.504(f)(2)(ii), and that the Employer agrees to the conditions of disclosure set forth in Section \_.06

**IN WITNESS THEREOF**, the party or parties hereto have executed this amendment by its duly authorized officer as of this \_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_, 2004.

**(Name of Employer)**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Witness:

Attest: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SUMMARY OF MATERIAL MODIFICATIONS**

To: Employee Participants in the *[Insert Name of the Plan],* and COBRA Participants

From: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The [*Insert Name of Plan*] sponsored by [*Insert Name of Employer*] as been revised. All of the changes summarized below are effective as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***.***

**PRIVACY RIGHTS**

**What disclosures of enrollment/disenrollment information are permitted?**

The Plan may disclose to the Employer information on whether you are participating in the Plan, or are enrolled in or have disenrolled.

**What uses and disclosures of summary health information are permitted?**

The Plan may disclose Summary Health Information to the Employer, provided the Employer requests the Summary Health Information for the purpose of (a) obtaining premium bids from health plans for providing health insurance coverage under the Plan; or (b) modifying, amending, or terminating the Plan.

“Summary Health Information” means information that (a) summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the Employer had provided health benefits under the Plan; and (b) from which the information has been deleted, except that the geographic information need only be aggregated to the level of a five-digit zip code.

**What required uses and disclosures of PHI are permitted for plan administrative purposes?**

Unless otherwise permitted by law, and subject to the conditions of disclosure and obtaining written certification, the Plan (or an Insurer on behalf of the Plan) may disclose PHI to the Employer, provided the Employer uses or discloses such PHI only for Plan administration purposes. “Plan administration purposes” means administration functions performed by the Employer on behalf of the Plan, such as quality assurance, claims processing, auditing, and monitoring. Plan administration functions do not include functions performed by the Employer in connection with any other benefit or benefit plan of the Employer, and they do not include any employment related functions.

Notwithstanding the provisions of this Plan to the contrary, in no event shall the Employer be permitted to use or disclose PHI in a manner that is inconsistent with federal regulations.

**Under what conditions can PHI be are disclosed for plan administration purposes?**

The Employer agrees that with respect to any PHI (other than enrollment/disenrollment information and Summary Health Information, which are not subject to these restrictions) disclosed to it by the Plan (or an Insurer on behalf of the Plan) the Employer shall:

* Not use or further disclose the PHI other than as permitted or required by the Plan or as required by law.
* Ensure that any agent, including a subcontractor, to whom it provides PHI received from the Plan agrees to and complies with the same restrictions and conditions that apply to the Employer with respect to PHI.
* Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Employer.
* Report to the Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware.
* Make available PHI to comply with HIPAA’s right to access in accordance with federal regulations.
* Make available PHI for amendment and incorporate any amendments to PHI in accordance with federal regulations.
* Make available the information required to provide an accounting of disclosures in accordance with federal regulations.
* Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of Health and Human Services for purposes of determining compliance by the Plan with HIPAA’s privacy requirements.
* If feasible, return or destroy all PHI received from the Plan that the Employer still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
* Ensure that the adequate separation between Plan and Employer (i.e., the “firewall”), required in federal regulations, is satisfied.

**Who is permitted to disclose Information?**

The Employer shall allow those classes of employees or other persons in the Employer’s control designated by the Employer to be given access to PHI. No other persons shall have access to PHI. These specified employees (or classes of employees) shall only have access to and use PHI to the extent necessary to perform the plan administration functions that the Employer performs for the Plan. In the event that any of these specified employees do not comply with the provisions of this Section, that employee shall be subject to disciplinary action by the Employer for non-compliance pursuant to the Employer’s employee discipline and termination procedures.

**When can PHI be disclosed to the Employer?**

The Plan shall disclose PHI to the Employer only upon the receipt of a certification by the Employer that the Plan has been amended to incorporate the provisions of federal regulations, and that the Employer agrees to the conditions of disclosure set forth in this summary.

Please attach this Summary of Material Modifications to your Summary Plan Description for future reference.

Please contact me, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (acting on behalf of the plan administrator, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_), if you have questions regarding the information in this Summary of Material Modification, or if you need another copy of the Summary Plan Description or the Certificate of Insurance booklet.

I can be reached at (----) -------- -------. Or you can write me at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attention: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

ERISA Information:

Plan Sponsor: \_\_\_\_\_\_\_\_\_\_\_

Sponsor’s EIN: \_\_-\_\_\_\_\_\_\_

Plan Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plan Number: 50\_

Plan Year: \_\_\_\_\_\_\_\_\_\_

**HIPAA TRAINING ACKNOWLEDGMENT**

I, the undersigned employee of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (the “Employer”) make the following certifications and representations:

a)     I have attended an HIPAA Privacy Policy presentation; and

b)     I have read the Employer’s Privacy Policies and Procedures, understand their terms, and agree to be bound by them; and

c)      I acknowledge that compliance with HIPAA and Employer’s Privacy Policies and Procedures is a material condition of my employment and that my failure to comply with them could result in disciplinary action.

My Name :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

My Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Today’s Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

As a representative of the Employer, I acknowledge the receipt of this acknowledgment as of the above date.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**REQUEST FOR ALTERNATE COMMUNICATIONS**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**I. Request for Restriction**

I hereby request that I receive communications of my protected health information from any of the following plans sponsored by\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Employer”) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(the “Plans”), as follows:

Specifically, I request that the following communications be subject to the above request:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Alternative means of contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*\*The disclosure of all or part of the information to which this request pertains could endanger me.

**II. Other Important Information**

I understand that the Plans will agree to all reasonable requests, but may condition this accommodation on, when appropriate, information as to how payment, if any, will be handled; and my specifying above an alternative means of communication.

**III. Signature of Individual or Individual’s Representative**

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

**Signature of individual or individual’s representative Date**

*(Form MUST be completed before signing.)*

Printed name of the individual’s personal representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Relationship to the individual, including authority for status as representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**I. Request for Accounting**

I hereby request an accounting of disclosures of my protected health information (PHI) in a “designated record set” held by the any of the following plans sponsored by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the (“Employer”) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Plans”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). Please provide an accounting of disclosures of PHI that occurred during the following period:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I understand that the Plans is not required to provide an accounting of disclosures of PHI made (1) to carry out treatment, payment or health care operations; (2) to me; (3) incident to a use or disclosure otherwise permitted or required by HIPAA; (4) pursuant to an individual authorization; (5) to certain persons involved in my care or payment for that care or to notify certain persons of my location, general condition, or death, or to assist in disaster relief efforts; (6) for specific national security or intelligence purposes; (7) to correctional institutions or law enforcement when the disclosure was permitted without authorization; (8) as part of a “limited data set” (as defined in HIPAA), which largely relates to research purposes; or (9) prior to the compliance date of April 14, 2004.

I understand that the accounting will include disclosures of PHI that occurred during the six years (or such shorter time period, if applicable) prior to the date of this request, including disclosures to or by business associates of the Plans. Except as otherwise provided below, for each disclosure, the accounting will include:

* the date of the disclosure;
* the name of the entity or person who received the PHI and, if known, the address of such entity or person;
* a brief description of the PHI disclosed; and
* a brief statement of the purpose of the disclosure that reasonably informs me of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for disclosure.

If the Plans made a disclosure over a period of time, the accounting may state the range of dates during which the disclosure was made. If a disclosure is routinely made within a set period after an event, the accounting may state the date of the event and the normal period within which the disclosure is made.

**II. Other Important Information**

If during the period covered by the accounting the Plans has made multiple disclosures of PHI to the same person or entity for a single purpose, that accounting may, with respect to such multiple disclosures, provide the above-referenced information for the first disclosure, with the frequency, periodicity or number of the disclosures made during the accounting period, and the date of the last disclosure.

If during the period covered by the accounting the Plans make its records available over a discrete period of time, the accounting may include the range of dates (e.g., access was provided from August 1 to August 3, 2004; or during the week of August 10, 2004). Alternatively, if the disclosure is routinely made within a set period of time from an event, the accounting may provide the date of the event and the normal interval.

If during the period covered by the accounting the Plans has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to the disclosures for which my PHI may have been included, provide certain information as permitted by HIPAA. If the Plans provide an accounting for such research disclosures, and if it is reasonably likely that my PHI was disclosed for such research activity, the Plans shall, at my request, assist in contacting the entity that sponsored the research and the researcher.

I understand that the Plans have 60 days to respond to this request. If the Plans are unable to take action within the applicable time period, the Plans may extend the time for such action by 30 days, provided that the Plans, within the applicable time period, give me a written statement of the reasons for the delay and the date by which the Plans will complete its action on the request.

❏ If this request is for a second or subsequent accounting within a 12-month period, I agree to pay a reasonable, cost-based fee for the accounting.

**III. Signature of Individual or Individual’s Representative**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

**Signature of individual or individual’s representative Date**

*(Form MUST be completed before signing.)*

Printed name of the individual’s personal representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Relationship to the individual, including authority for status as representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**REQUEST TO AMEND OR CORRECT**

**PROTECTED HEALTH INFORMATION**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**I. Request for Amendment or Correction**

I hereby request to amend protected health information (“PHI”) about me in a “designated record set” held by one of the flowing plans sponsored by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Employer”) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Plans”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).

For purposes of this form, a *“designated record set”* is a group of records maintained by or for the Plans including enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used by or for the Plans to make decisions about individuals. The term “record” means any item, collection or grouping of information that includes protected health information that is maintained, collected, used or disseminated by or for the Plans.

**Describe Amendment Requested:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reason for Requested Amendment:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I understand that if the protected health information was not created by the Plans, the Plans are not required to honor my request. For example, if the information I wish to amend is in a medical report created by my health care provider, I must ask the provider to amend the report. I also understand that if the information is not available for my inspection, is not part of the Plans’ designated record set or is already accurate and complete, I cannot amend the information.

**II. Other Important Information**

I understand that the Plans will respond to my request within 60 days. If the Plans are unable to take action within the applicable time period, the Plans may extend the time for such action by 30 days, provided the Plans, within the original 60-day time period, gives me a written statement of the reasons for the delay and the date by which it will complete its action on the request.

If the Plans accept the requested amendment, the Plans shall make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise provided a link to the location of the amendment. The Plans shall timely inform me that the amendment is accepted and obtain my identification of relevant persons with which the amendment needs to be shared as provided in HIPAA. The Plans shall make reasonable efforts to inform (a) persons identified by me as having received my PHI and needing amendment, and (b) persons, including business associates (as defined in HIPAA) of the Plans, that the Plans know have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information.

If the request is denied in whole or in part, the Plans will provide me with a written denial

**III. Signature of Individual or Individual’s Representative**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

**Signature of individual or individual’s representative Date**

*(Form MUST be completed before signing.)*

Printed name of the individual’s personal representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Relationship to the individual, including authority for status as representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**REQUEST TO INSPECT OR COPY**

**PROTECTED HEALTH INFORMATION**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**I. Request to Inspect or Copy Protected Health Information**

I hereby request to review protected health information (PHI) about me in a “designated record set” held by one of the plans sponsored by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Employer”) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(the “Plans”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

For purposes of this form, a “*designated record set”* is a group of records maintained by or for the Plans including enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used by or for the Plans to make decisions about individuals. The term “record” means any item, collection or grouping of information that includes PHI that is maintained, collected, used or disseminated by or for the Plans.

Check any of the below, as applicable:

❏ I want to inspect PHI about myself maintained in the designated record set.

❏ I want to obtain a copy of PHI about myself that is maintained in the designated record set.

❏ I request that a copy of PHI about myself be mailed to the following address:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

❏ I request that a copy of PHI about myself be mailed to the designated person (other than myself) at the following address:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

❏ I request that the information be provided in the following format: (circle one)

Paper Computer Disk CD ROM E-Mail

❏ I request that the information be provided electronically as follows: (circle one)

Word Excel text HTML text-based PDF Other: (Specify)

I understand that if the format requested is not readily producible, the Plans will provide a readable hard copy form or such other form or format as agreed to by the Plans and by me.

I do/do not (circle one) agree that the Plans may provide a summary of the health information instead of allowing me to review the information.

*If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Plans will only produce the PHI once in response to a request.*

**II. Other Important Information**

I understand that the Plans have 30 days to respond to this request. If the Plans are unable to take action within the applicable time period, they may extend the time for such action by 30 days, provided that the Plans, within the applicable time period, give me a written statement of the reasons for the delay and the date by which the Plans will complete its action on the request. I understand that if the Plans grant this request, in whole or in part, it will inform me of the acceptance of this request and provide the access requested. In that event, the Plans will arrange with me for a convenient time and place to inspect or copy the PHI, or it will provide me with a copy as I have requested. However, if the Plans deny the request, in whole or in part, it will provide me with a written denial.

I agree to pay any fees for copying, summarizing, or explaining my health information. Fees will be reasonable and cost-based and will include only the cost of copying, postage (if I request that a copy or summary be mailed), and preparation of a summary (if I agree to a summary). If the information is requested in electronic form, the fee for providing such may include labor costs involved in producing the information and any cost for supplies needed to comply with the request.

I understand that this request does not apply to certain health information, including (1) information that is not held in the designated record set; (2) psychotherapy notes; (3) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and (4) other health information not subject to the right to access information under HIPAA.

**III. Signature of Individual or Individual’s Representative**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_

**Signature of individual or individual’s representative Date**

*(Form MUST be completed before signing.)*

Printed name of the individual’s personal representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Relationship to the individual, including authority for status as representative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_