# 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.

<u>Minimum-Necessary Standard</u>

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 officer responsible for the development and implementation of privacy policies and procedures and a contact person (the privacy officer 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 HIPAA 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.