HIPAA Privacy Summary

Kelly McLendon, RHIA

This document is intended to summarize the latest HIPAA Privacy Rules in a format that is understandable by record managers and all of the stakeholders of protected health information.

Every Covered Entity (CE) or Business Associate (BA), Health Information Exchange (HIE) or PHR (Personal Health Record) that is subject to HIPAA Rules must be proactive and in creating, implementing and maintaining the processes surrounding HIPAA Privacy and Security. The enforcement of the HIPAA Rules begins in February 2010 and is excepted to rise significantly compared with past enforcement efforts.

All entities that fall under HIPAA jurisdiction must also be aware of and follow the State Laws, Rules and Regulations that are applicable as well. HIPAA provides a 'floor' of regulation; if State Law (Rule or Regulation) is stronger then it may apply instead). However, following HIPAA standards is generally recommended as a good benchmark of best practice.

HIPAA Breach Notification Interim Final Rule Summary

The American Recovery and Reinvestment Act of 2009 ("the Act") made several changes to the HIPAA privacy rules—including adding a requirement for notice to affected individuals of any ***Breach* of *unsecured* protected health information (PHI)**. On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule (the "Rule") that lays out the specific steps that HIPAA-covered entities and their business associates must take. While this Rule, which became effective September 23, 2009, is technically in effect, HHS has stated that while it expects covered entities to comply with this Rule as of September 23, it will not impose sanctions for failure to provide the required notifications for Breaches discovered through February 22, 2010. Instead, during such period it will work with covered entities to achieve compliance through technical assistance and voluntary corrective action. This language illustrates that Covered Entities (CE) and Business Associates (BA) must update their privacy compliance programs and processes in 2009 and early 2010, before enforcement begins. HHS appears to assume the position that compliance audits and complaint investigation will take into account efforts made by the CE and BA to be compliant with the Rules and to effectively be pro-active in regards to PHI Privacy and Security.

This notification summarizes the notice provisions of the Rule so that you can understand the need for to instituted the correct processes in the case of a discovered Privacy Event or a suspected **Breach of unsecured protected health information**.

For purposes of compliance please assume all specific patient information (PHI) to which properly authorized personnel have access is (1) unsecured protected health information and that (2) any Breach is to be reported to appropriate parties within your organization. These parties will log the Event and make determinations on the notification and remediation / corrective action steps to be undertaken.

Privacy Events, Breaches and HIPAA Violations

There is no concept of Privacy Events in the HIPAA Rules, however this is a crucial concept that helps to frame the process necessary for CEs and BAs to follow when investigating and determining HIPAA Violations and Breaches. Kelly McLendon defines Privacy Events as the 'discovery of incident(s) related to the acquisition, access use and disclosure of an individual's PHI that upon further investigation may or may not be deemed HIPAA Privacy violations or Breaches of unsecured PHI'. Privacy Events are a non-prejudicial designation for incidents that have occurred but have not yet been determined to be violations of Breaches. Breaches of unsecured PHI and HIPAA violations are determinations made by the CE and / or BA in the estimation of those parties as they work to apply the elements of the Rules to their own environment.

The new Privacy requirements apply if all of the following are present in a Privacy Event:

- **There is a "Breach."** The Rule defines "Breach" to mean (subject to certain exceptions) the unauthorized acquisition, access, use, or disclosure of protected health information ("PHI").
- **The PHI is "unsecured."** The Rule defines "unsecured protected health information" to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.
- **The Breach "compromises the security of the PHI."** Under the Rule, this occurs when there is a significant risk of financial, reputational, or other harm to the individual who's PHI has been compromised.

HIPAA Privacy Rule General Information

- Breach notification documents for patients must be in plain, reasonable language.
- Notice of Breaches must be sent to next of kin if the patient has expired.
- Don't sent Breach notices from both CE and BA, no multiple notices. Same is true for HIPAA and FTC notices for PHR's.
- CE's and BA's must develop and document Policies and Procedures, train workforce members, have sanctions for failure to comply, require CE to refrain from intimidation or retaliatory acts.
- CE's and BA's must develop and document Policies and Procedures, train workforce members, have sanctions for failure to comply and require the CE to refrain from intimidation or retaliatory acts.

Notification Requirements to Individuals and /or Media in the Event of a Breach of Unsecured PHI

The Breach notifications required by the recent legislation and the Rule are significant and are triggered by the "discovery" of the Breach of unsecured PHI. A Breach is treated as "discovered" by a covered entity as of the first day the Breach is known, or reasonably should have been known, to the covered entity. Individuals, and at times the media, must be notified of certain Breaches of unsecured PHI. This is a very serious process with potential legal and regulatory consequences that illustrate the need for very careful reporting and HIPAA Rule compliance in order to minimize the liabilities and risks to your organization.

Notification as provided below must be undertaken by appropriate parties within your organization

- **Notification to Individuals.** A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach, without unreasonable delay and in no case later than 60 calendar days after the date the Breach was first discovered by the covered entity.
- **Notification to Media.** If a covered entity discovers a Breach affecting 500 or more residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the Breach was discovered by the covered entity.
- **Notification to HHS.** If 500 or more individuals are involved in the Breach, then the covered entity must notify HHS concurrently with the individual notifications. While we have never had a Breach involving this number of patients, we ask you be especially aware that such a Breach may occur.
    - For Breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such Breaches and annually submit such log to HHS. We have maintained such a log and will now be required to submit that log annually to HHS.

HHS (through the HHS enforcement agency; The Office of Civil Rights or 'OCR') requires annual notification for Breaches involving less than 500 individuals per Event annually. If a Breach involves more than 500 individuals it must be reported within the 60 day mandatory reporting period.

The link for submitting a Notice of Breach to OCR is as follows:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/Breachnotificationrule/brinstruction.html

Notices should be submitted on routinely annually before March 1 of the following year. For Example breach Notification to OCR for the period for Breaches involving <500 individuals ending 2009 (reporting requirement commenced with Rule publication; dates for reporting are September 23 – December 31) is due March 1, 2010. In order to comply with these Rules detailed logging of all privacy Events and Breaches is required.

Workforce Training and Complaints

Further, the Rule requires that Covered Entities must **train** all members of its work force on these matters, provide a **process for individuals to make complaints**, refrain from taking retaliatory acts against those who do complain and to develop and impose appropriate **sanctions** for members of its workforce who fail to comply with the HIPAA Privacy Rule provisions.

OCR website for Privacy complaints (http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html)

What is Secured PHI?

On April 27, 2009, HHS issued the HITECH Breach Notification Guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. That guidance creates a safe harbor so that covered entities and business associates would not be required to provide the Breach notifications required by the Act for PHI meeting these standards. PHI is

rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following methods are used:

(1) *Encryption*. Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean 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. The Rule identifies the various encryption processes which are judged to meet this standard. Further, such confidential process or key that might enable decryption must not have been Breached. To avoid a Breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) *Destruction*. Hard copy PHI, such as paper or film media, is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Other important points about HIPAA Security:

- Encryption and specified destruction are not the only means of compliance with the HIPAA Security Rule; however they are key to understanding if a Breach of 'unsecured' PHI has occurred. Encryption of data in any of its states is highly desired to prevent Breach Notification from being necessary.
- Access controls alone are not enough, if access controls are utilized alone to provide security for PHI and there is a Breach (wrongful disclosure), Notification *is* required.
- Paper redaction does not exempt Breach but can be used to render PHI non-PHI. Once patient information is no longer PHI (linked to the patient) Breach notification is not applicable.
    - 18 identifiers comprise de-identification and must be considered in order to render PHI into non-PHI.
- Encryption keys should be kept on separate devices from data when used to create secured PHI.

Determining Whether a Breach of Unsecured Protected Health Information Has Occurred

The Rule envisions that Covered Entities and their Business Associates will analyze the following in determining whether a Breach of unsecured PHI has occurred:

(1) Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule. For an acquisition, access, use, or disclosure of PHI to constitute a Breach, it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified in accordance with 45 CFR 164.514(b), it is not PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a Breach under the notification requirements of the Act and the Rule.

(2) Analyze whether there is a use or disclosure that compromises the security and privacy of PHI (Harm Threshold Analysis). HHS clarifies that a use or disclosure that "compromises the security and privacy of PHI" means a use or disclosure that "poses a significant risk of financial, reputational, or other harm to the individual." Thus, in order to determine whether a Breach has occurred, Covered Entities and Business Associates will need to conduct a risk assessment (which may be referred to as a Harm Threshold Analysis) to determine whether the potential Breach presents a significant risk of harm to individuals as a result of an impermissible use or disclosure of PHI. The Rule provides a number of

factors which should be taken into account when conducting a risk assessment. A Covered Entity should consult its legal counsel with respect to the impact of the presence of such factors.

(3) Assess Whether any Exceptions to the Breach Definition Apply. The Rule discusses a number of exceptions to the definition of Breach. The following three situations are excluded from the definition of "Breach" under the Act:

(i) The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

(ii) The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at a organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

(iii) An unauthorized disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

The covered entity or business associate has the burden of proving why a Breach Notification was not required and must document why the impermissible use or disclosure fell under one of the exceptions. Covered entities should document the risk and other Breach assessments accordingly.

Notification Requirements to Individuals and /or Media in the Event of a Breach of Unsecured PHI

The Breach notifications required by the Act and the Rule are significant and are triggered by the "discovery" of the Breach of unsecured PHI. A Breach is treated as "discovered" by a covered entity as of the first day the Breach is known, or reasonably should have been known, to the covered entity. Given that knowledge of a Breach may be imputed, a covered entity should implement reasonable Breach discovery procedures.

- **Notification to Individuals.** A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach, without unreasonable delay and in no case later than 60 calendar days after the date the Breach was first discovered by the covered entity. The Act and the Rule specify the content requirements and the methodology required for providing such Breach notices. For covered entities that do not have sufficient contact information for some or all of the affected individuals, the Rule requires that substitute notice be provided as soon as reasonably possible. If a covered entity has insufficient contact information for 10 or more individuals, then substitute notice must be provided via a posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside. In such instances, the covered entity is also required to have an active toll-free number for 90

days so that an individual can find out whether his or her unsecured PHI may be included in the Breach.

- **Notification to Media.** If a covered entity discovers a Breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the Breach was discovered by the covered entity. *Note – we will work on the premise, that the rule should read 500 or more.*
- **Notification to HHS (OCR).** If more than 500 individuals (are involved in the Breach, regardless of whether the Breach involved more than 500 residents of a particular State or jurisdiction, then the covered entity must notify HHS concurrently with the individual notifications. *Note – we will work on the premise, that the rule should read 500 or more.*
    - For Breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such Breaches and annually submit such log to HHS. For calendar year 2009, the covered entity is only required to submit the log for Breaches occurring on or after September 23, 2009.
- **Notification by a Business Associate.** Following the discovery of a Breach of unsecured PHI, a business associate is required to notify the covered entity of the Breach so that the covered entity can, in turn, notify the affected individuals. To the extent possible, the business associate should identity each individual whose unsecured PHI has been, or is reasonably believed to have been, Breached. Such notice should be given without unreasonable delay and no later than 60 days following discovery of a Breach.
- **Delay Required by Law Enforcement.** The Act provides that a Breach notification may be delayed if a law enforcement official determines that such notification would impede a criminal investigation or cause damage to national security.
- **Methods of notification include:**
    - First class mail to last known address
    - Or e-mail if preferred by patient
    - Provide for substitute notice if insufficient or unknown contact information
    - In the case of a Breach with 10 or more patients with unknown contact info post general info in media, site website and have a toll free number to call
- **Contents of Breach Notification:**
    - Dates of Breach and Discovery
    - Brief description of what happened
    - Description of types of information involved
    - Steps individuals should take to protect themselves
    - Brief description of CE (or BA) remediation actions
    - Contact information for individuals to learn more
- **Timing of notification:** Without unreasonable delay, not longer than 60 days after discovery

Interaction of Interim Final Rule with FTC, HIPAA Rules, and Other State Laws

On August 17, 2009, the FTC issued companion Breach notification requirements for vendors of personal health records (PHRs) and their third party service providers following the discovery of a Breach of unsecured PHR identifiable health information. Entities operating as HIPAA-covered entities and business associates are not subject to these FTC Breach notification rules. But in certain instances where a Breach involves an entity providing PHRs to customers of HIPAA-covered entity through a business associate arrangement, and directly to the public, the FTC will deem compliance with the HHS Rule as compliance with its own Breach notification rules.

HHS has emphasized that this Rule does not modify a covered entity's responsibilities with respect to the HIPAA Security Rule; nor does it impose any new requirements upon covered entities to encrypt all PHI. A covered entity may still be in compliance with the Security Rule even if it decides not to encrypt electronic PHI so long as it utilizes another method to safeguard information in compliance with the Security Rule. However, if such method is not in compliance with the requirements of the Rule with respect to securing PHI, then the covered entity will be required to provide a Breach notification to affected individuals upon a Breach of unsecured PHI. The Rule preempts contrary State Breach notification laws. A covered entity must still comply with requirements of State law which are in addition to the requirements of the Rule, but not contrary to such requirements (such as additional elements required to be included in a notice).

Enforcement

Enforcement and Penalties begins February 2010. The Department of Health and Human Services has moved enforcement authority for the HIPAA Security Rule to the HHS Office for Civil Rights (OCR), this means more effective enforcement of both HIPAA Privacy and Security. There is projected to be increased enforcement from OCR. There has been an upswing in their recruitment of OCR enforcement agents. That along with mandates within HITECH (the portion of ARRA that covers HIPAA expansion) for OCR to perform on-going (random) Privacy and Security checks it is apparent that all CEs and BAs to need to be very proactive in their management of Breach detection and notification.

In the past CMS (Centers for Medicare and Medicaid Services) has enforced HIPAA Security Rules while OCR has handled Privacy Rule compliance. The move to combine Privacy and Security enforcement under one agency (OCR) will eliminate duplication of work and increase efficiency according to the HHS Secretary. The other significant enforcement change is that under HITECH State Attorney Generals can now bring actions for Privacy violations in federal court.

In regards to enforcement, rules were issued in October 2009 that raised the maximum amount of fines that can be levied in a single year. The Interim Final Rule Related to HIPAA Enforcement Under HITECH; Federal Register/Vol. 74, No. 209/Friday, October 30, 2009/Rules and Regulations proscribes the below listed penalties for HIPAA violations.

This Rule raises the penalties for violations to a max of $1.5 million in any single year for repeated, similar violations. Also the Rule clarified that CE's and BA's could be fined for violations that they did not know about.

CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

- (A) Did Not Know – $100–$50,000 (each violation) up to $1,500,000
- (B) Reasonable Cause - $1,000–50,000 (each violation) up to $1,500,000
- (C)(i) Willful Neglect - Corrected - $10,000–50,000 (each violation) up to $1,500,000
- (C)(ii) Willful Neglect - Not Corrected - $50,000 (each violation) up to $1,500,000

State Attorney Generals are authorized to bring civil actions in federal Court under HIPAA and it is expected that the addition of State enforcement will significantly increase the amount of enforcement activities and liabilities for all healthcare providers that do not strictly follow these rules.

References:

1. Art Louv, Esquire; Physician Associates LLC\HIPAA & Red Flag Rules\HIPAA\PAL Summary HIPAA Breach Notification Interim Final Rule revised 08.24.09. updated 11.13.09.doc

2. ARRA / HITECH Act February 17, 2009

3. HHS Interim Final Rule Breach Notification for Unsecured Protected Health Information Effective September 23, 2009

DEPARTMENT OF HEALTH AND HUMAN SERVICES
45 CFR Parts 160 and 164
RIN: 0991-AB56
Breach Notification for Unsecured Protected Health Information

4. Office of Civil Rights website;

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

5. Federal Register/Vol. 74, No. 79/Monday, April 27, 2009/ Rules and Regulations Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009

6. NIST Special Publication 800-66 Revision 1; An Introductory Resource Guide for Implementing the HIPAA Security Rule