Assessment of Interim Final HHS Breach Notification Rule for Electronic Health Records

Compliance Requirements

August 19, 2009

Introduction

On August 19, 2009, Health and Human Services (HHS) published the interim final rule for breach notification of individuals affected by an unauthorized disclosure of individually identifiable health information that is protected health information (PHI) held in an Electronic Health Record (EHR). This interim final rule addresses related breach notification provisions of the American Recovery and Reinvestment Act (ARRA) of 2009. The rule has an effective date 30 days after publication, but HHS has indicated that they will decline to enforce the regulation until 180 days after publication to allow organizations affected by the regulation to come into full compliance.

Within the same rule publication, HHS also issued updated guidance related to technical security measures for appropriately securing electronic protected health information. For those providers and their business associates who follow this guidance, compliance with the guidance creates a safe harbor under the HHS breach notification rule from the notification requirements under the rule in the event of a breach.

Summary

The following are the key points for attention for the requirements of the final rule and its applicability to Cerner’s solutions, services and operations.

- The compliance date of the rule is 30 days after its publication to the federal register (September 2009), but HHS has indicated they will not enforce the rule until February 2010 to allow regulated entities time to come into compliance
- The rule as final applies only to breaches that involve the unauthorized acquisition, access, use or disclosure by unauthorized individuals of unsecured PHR identifiable health information
  The basis for determining unauthorized use or disclosure is if the purpose of the use or disclosure is a violation of the HIPAA Privacy Rule’s provisions for permissible use or disclosure
  Unsecured is defined as PHI that has not been secured by technical security measures outlined in the Secretary of Health and Human Services (HHS)
guidance issued April 17, 2009 as updated in this interim final rule – a link to this guidance is available in the Reference section of this whitepaper

- The rule directly impacts HIPAA covered entities and by extension lays out requirements for business associates as well

- The rule creates breach notification requirements as to timeliness, content and method both to the individual and to HHS

- Cerner will bear responsibilities as a business associate as described in this whitepaper to help its clients comply with this rule for breaches discovered by Cerner acting as a business associate

  Cerner as a covered entity (e.g. Cerner’s health plan, Cerner’s Health Care Clinic) will bear the covered entity responsibilities as described in this whitepaper

- Covered entities and business associates will bear specific additional policy and procedure requirements, training requirements and compliance requirements for the breach provisions of this rule

**Impact on Cerner and Cerner’s Clients**

The impact of the final rule on Cerner can be summarized in the following manner:

- Cerner meets the rule’s definition both as a business associate and a covered entity as HIPAA defines them in different contexts of operation

  - Cerner is a business associate in all of its operations that involve consulting services, support services, transaction services and hosting or management services for clients who are covered entities under HIPAA

  - Cerner is a covered entity for its operations that involve the Cerner associate health plan and the Cerner Health Care Clinic

The rule only has applicability on Cerner if Cerner fails to appropriately employ technical security measures as suggested in the guidance issued by the Secretary of HHS as is mentioned within this whitepaper, and breaches involving PHI as defined within this whitepaper occur.

**What Is In The Final Rule?**

The final rule has several key sections in which HHS outlines what kinds of entities are covered by the rule, what constitutes a breach, what processes, content and timeliness of notice are required for administering a breach notification, and what kinds of guidance should be given to consumers who are affected by a breach.

HHS also devotes considerable comment to grounding that what constitutes an unauthorized use or disclosure in the requirements found within the HIPAA Privacy rule.

**Compliance Date**

The rule has an effective date 30 days after publication to the federal register, but HHS has indicated they will not take enforcement action until February, 2010 – 180 days after publication.

**Key Definitions and Requirements Related to Identifying a Breach of Privacy**

The interim final rule lays out some key definitions and related requirements for covered entities and business associates to identify a breach, to assess if significant harm may result from the breach and what data constitutes protected health information that may be subject to a breach. These circumstances go well beyond the treatment given to breach in the FTC final rule for breaches from Personal Health Records (PHRs) because HHS is grounding the definition and circumstances of breach under the requirements of the HIPAA Privacy Rule.
1. Breach – the interim final rule defines a breach as “the acquisition, access, use or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information” The subpart E reference is the HIPAA Privacy Rule. HHS is placing a breach in the frame of reference that it must be a use or disclosure for a purpose not permitted under the HIPAA Privacy rule in order to be considered breach. A covered entity bears the burden of determining if a breach has occurred and if significant harm may result to the individual affected by the breach. HHS offers the following guidance to determining if a breach has occurred, and how to ascertain if significant harm has resulted:
   a. Is the use or disclosure of protected health information in question impermissible under the Privacy Rule?
      i. Uses or disclosures that violate minimum necessary requirements may constitute breach
      ii. Uses or disclosures that are incidental to an otherwise permissible use or disclosure do not constitute violations of the Privacy Rule
      iii. Violations of administrative requirements such as a lack of training or lack of security safeguards do not themselves qualify as potential breaches
   b. Does the use or disclosure compromise the security or privacy of the protected health information?
      i. This means that the incident poses significant risk of financial, reputational or other harm to the individual
      ii. The determination of significant risk requires the covered entity (and business associate) to conduct a risk assessment of the incident
   c. Did immediate steps to mitigate eliminate or reduce the risk of harm to less than a “significant risk”? If so, no breach has occurred. The burden of proof of this is upon the covered entity and its business associates.
      i. Steps may include recovery of lost devices containing protected health information or verifying that unintended recipients of protected health information return or destroy the information without accessing it or further using or disclosing it
   d. Did the information used or disclosed pose a significant risk of harm due to the incident? This part of the assessment needs to be fact specific – for example, HHS offered the following
      i. Limited information such as disclosure of a name of a patient and the dates of an admission absent any other information may not pose a significant risk
      ii. Disclosure of information about the services received by the patient would pose a significant risk
   e. Did the breach fall under one of the three exceptions provided for by the statute (see Exceptions to Breach below)?

2. Protected Health Information – the interim final rule defines protected health information as individually identifiable health information transmitted or maintained in any form or medium, including electronic information. De-identified information is not considered protected health information. The limited data set as defined by the Privacy Rule is considered protected health information.
   a. One exception to the use or disclosure of the limited data set is that if the limited data set excludes the 16 direct identifiers as well as dates of birth and zip codes then unauthorized use or disclosure of the resulting data set would not be considered a breach

3. Unauthorized Acquisition, Use or Disclosure – Unauthorized means an impermissible use or disclosure of protected health information under the HIPAA Privacy Rule. A violation of the HIPAA Security Rule (e.g. through a failure to comply with a mandatory requirement such as auditing or use of access controls) is not considered a potential breach although it could create a vulnerability that could lead to a breach.

4. Exceptions to Breach – HHS outlines three circumstances that are exceptions to breach as defined by ARRA 2009 – and the covered entity or business associate has the burden of proof to show why breach notification is not required if the breach falls under one of these exceptions
a. If the unauthorized acquisition, access or use of protected health information was unintentional and made by an employee or individual acting under the authority of a covered entity of business associate, was made in good faith and within the course and scope of employment and does not result in further use or disclosure
b. If the inadvertent disclosure of PHI was from one person authorized to access PHI at a covered entity or business associate to another individual authorized to access PHI at the covered entity or business associate, and did not result in further use or disclosure
c. If the unauthorized disclosure to an unauthorized person would be one where the unauthorized person could not reasonably have retained the information

5. Business Associate – the FTC uses the HIPAA definition of a business associate
6. HIPAA Covered Entity – the FTC uses the HIPAA definition of a covered entity (health care provider, clearinghouse for purpose of HIPAA EDI or a health plan
7. Unsecured – unsecured means not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS) in guidance issued under ARRA 2009 to address the definition of unsecured protected health information – this guidance issued by the Secretary on April 17, 2009, may be found at -
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/hitechrfi.pdf - this guidance was updated on August 19, 2009, and the updated guidance may be found in the same document as the interim final rule – see Reference section below
a. The guidance suggests encryption is required to prevent an entity subject to this regulation from falling within the scope of the definition of “unsecured” – the guidance creates a safe harbor of sorts for a regulated entity in the event of a loss or breach from the reporting requirements of this final regulation
b. The encryption requirement applies to data as stored on any manner of portable computing device or removable media, as held in databases or on end user computing devices and as may be communicated and in transit to or from the PHR

Scope of Regulation

HHS has regulatory authority over medical records maintained in paper or electronic form that contain individually identifiable protected health information as maintained by HIPAA covered entities and their business associates.

The final rule focuses on breaches of “unsecured” individually identifiable PHI held in an electronic health record system. Unsecured has the meaning defined above. Breaches of PHI that is appropriately secured by means suggested by the Secretary of HHS’s guidance would not be considered within the scope of this interim final regulation. Breaches involving the use or disclosure of de-identified protected health information also would not be considered within the scope of this interim final rule.

Breach Notification Requirements

The breach notification requirements for unauthorized acquisition (possession or access) of unsecured individually identifiable PHI include the following:

Timeliness of Notice

1. Timely notification of the affected individual(s)
   a. A regulated entity must notify the affected individuals within 60 days of the day of discovery of the breach
      i. The notification should not await the completion of an investigation into the cause of the breach but proceed once the entity believes in good faith that it has identified affected customers
      ii. If additional affected individuals are identified beyond those initially identified close to the close of the 60 day window, the regulated entity may take additional
time within what is reasonable beyond 60 days to provide notification to those additional individuals

iii. The day of discovery will be considered the day that the covered entity comes to know of or reasonably should have known of the breach
   1. The day of discovery shall be the day that either the covered entity or business associate working on behalf of the regulated entity becomes aware of the breach
   2. The covered entity or business associate will be considered aware of a breach if any of its employees or agents is aware or reasonably should be aware of the breach

iv. Business associates must provide notice to the covered entity of any such breaches that they may become aware of
   1. The notice shall contain an identification of each affected individual

v. The concept of “reasonably should have known” means that HHS expects covered entities and business associates that collect and store PHI to maintain reasonable security measures including breach detection measures to assist in detecting breaches in a timely manner
   1. A covered entity or business associate that fails to employ such measures will be in violation of the regulation if a breach occurs

b. The notification must be timely in that it must occur without unreasonable delay from the date of discovery

c. The notification should be of any affected individuals who are patients of the covered entity or of those affected individuals whose records were maintained by a business associate of the covered entity

d. The notification requirement under the HHS rule does not apply to breaches involving PHRs offered by a PHR vendor or PHR related entity that is not offered by a HIPAA covered entity or business associate – the FTC breach notification rule applies in those cases
   i. PHR vendors or related entities are those entities that provide PHRs or related services directly to PHR customers without going through a HIPAA covered entity or business associate

e. Business associates must provide timely notice to the covered entity for breaches they discover
   i. This must be within the 60 calendar day period and be as soon as is reasonably practical once a breach is discovered
   ii. The business associate must provide information as to affected individuals, and as to the nature of the information subject to the breach and provide what is necessary to support the notification content
   iii. Business associates and covered entities may determine who is in the best position to provide notification to the individual

2. The notice should be administered by
   a. First class mail or by e-mail based on an individual’s meaningful choice as to the preference for receiving such notices considering what contact information is collected by the regulated entity
      i. If the affected individual is a minor or lacks legal capacity to receive the notice, the notice may be administered to the parent or personal representative of the affected individual
      ii. If the individual is deceased, the notice may be sent to the last known address of the next of kin or personal representative of the affected individual
   b. Substitute means if the covered entity does not have sufficient contact information or if some notices are returned as undeliverable – this may be by telephone or other means
      i. Alternatively, this may be by posting a notice on the web site of the covered entity
c. In the case of failure to reach ten or more affected individuals, the covered entity must provide notice through the home page of its web site or through major print or broadcast media
   i. Any method through a web site must be conspicuous and bear appropriate wording if through a link on the web site
      1. Such a notice must be left available for 90 days
   ii. Any method done through the media must consider how to reasonably reach the individuals affected, be plainly stated and run multiple times
3. In the case of a breach involving 500 or more individuals within any given state, notice must include general notice through media outlets in the area affected by the breach
   a. This is supplemental to the notice given on an individual basis
4. HHS must also be noticed within 60 calendar days of any breach involving over 500 individuals concurrent to notifying affected individuals
   a. This notice is required without regard to geographic jurisdiction (e.g. any breach involving over 500 individuals must be so reported even if it involves less than 500 individuals in any one state)
   b. If a breach involves less than 500 individuals, the regulated entity must maintain an entry in an annual log maintained on a calendar year basis and provide the log to HHS within 60 days of the end of the calendar year

Content of Notice

The notice must contain the following:

- A description of how the breach occurred
- The date of the breach and the date of the discovery of the breach if known
- The type of information (but not the specific PHI) involved in the breach
- Steps individuals should take to protect themselves from potential harm
  o These steps should be appropriate to the circumstance of the breach
    If for medical identity theft that may include requesting and reviewing medical records for error, monitoring explanations of benefits received from health insurers, following up with providers if billings are not received to determine if a billing address has been compromised and similar measures
    If the breach involves Social Security numbers, the covered entity should suggest steps to mitigate or prevent financial identity theft including placing a fraud alert on credit reports, obtaining and reviewing credit reports and contacting local law enforcement
- A description of what the affected covered entity is doing to investigate the breach, mitigate any losses and to protect against any further breaches
- Contact procedures for affected individuals to ask questions or learn additional information
- The notice must be in plain language at the appropriate reading level

Policy and Procedure Requirements of Covered Entities and Business Associates

Covered entities and business associates must

- Develop and document policies and procedures to address the above requirements
- Provide for workforce members to be appropriately trained on these policies and procedures
- Have sanctions for failure to comply with these policies and procedures
- Permit individuals to file complaints regarding these policies and procedures or a failure to comply with them
  o Require covered entities not to engage in intimidating or retaliatory acts
- Maintain documentation that all required notifications were made or alternatively of its risk assessment or the application of any exceptions to the definition of “breach” to demonstrate that notification was not required
Reference

The interim final rule may be accessed at the following location –


The original HHS guidance on appropriate technical security measures issued in April 2009 to guard against “unsecured PHI” may be found at:


The updated guidance is found within the interim final rule.

NIST documentation on encryption standards referenced by the HHS guidance may be found at:

http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf for data at rest and at
http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf and