Assessment of Final FTC Breach Notification Rule for Personal Health Records

Compliance Requirements

August 19, 2009

Introduction

On August 18, 2009, the Federal Trade Commission (FTC) published the final rule for breach notification of individuals affected by an unauthorized disclosure of individually identifiable health information held by a Personal Health Record (PHR) vendor or entity. This 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 the FTC 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.

Summary

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

- The compliance date of the rule is 30 days after its publication to the federal register (September 2009), but the FTC 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 acquisition by unauthorized individuals of unsecured PHR identifiable health information
  - Unsecured is defined as PHR identifiable health information that has not been secured by technical security measures outlined in the Secretary of Health and Human Services (HHS) guidance issued April 17, 2009 – a link to this guidance is available in the Reference section of this whitepaper
- The rule directly impacts entities that are in the role of a PHR vendor and a PHR related entity that provides services to the customers of the PHR vendor an organization
  - The rule does not apply to HIPAA covered entities or business associates – PHRs offered by such entities are subject to the breach notification rule issued by HHS on breaches from electronic health records systems
  - The rule indirectly applies to third party service providers who provide services to a PHR vendor or related entity such as hosting services for information technology
- The rule creates breach notification requirements as to timeliness, content and method both to the individual and to the FTC
The FTC has jurisdiction over PHRs since they are offered to the public as a consumer product that is marketed, sold and used across state lines
As long as Cerner in all of its roles (see next section) as a regulated entity appropriately secures PHR identifiable health information, it should not be subject to the breach notification requirements of the final rule if such information is acquired in an unauthorized manner

**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 PHR vendor and third party service provider
  - Cerner is a PHR vendor in the context of offering PHRs to Cerner associates through Healthe as an employer
  - Cerner is a third party service provider for its role in hosting PHRs offered by Cerner clients who are not HIPAA covered entities or business associates
- Cerner is also subject to the HHS rule on breach notification as a HIPAA business associate where the entity offering the PHR is itself a HIPAA covered entity

The rule as final 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.

**What Is In The Final Rule?**

The final rule has several key sections in which the FTC 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.

**Compliance Date**

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

**Key Definitions**

There are a number of key definitions in the final rule that set context for the regulation:

1. Breach of Security – the final rule defines a breach as “the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual”. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of PHRs, a PHR related entity or third party service provider that experienced the breach has reliable evidence showing that there has not been or could not reasonably have been any unauthorized acquisition of such information."
   a. The FTC defines acquisition as not only meaning that someone obtained information in an unauthorized manner, but also that unauthorized access to the information was possible such as in the case of a lost or stolen laptop or PDA that held such information on it
   b. A regulated entity may rebut that unauthorized acquisition could have occurred if they can produce reliable evidence that there had not been or reasonably could not have been an unauthorized acquisition such as by proving through forensic analysis that a file on a stolen laptop had not been opened
2. Business Associate – the FTC uses the HIPAA definition of a business associate
3. 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
4. Personal Health Record (PHR) – an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual”
5. PHR Identifiable Health Information – individually identifiable health information that is provided by or on behalf of an individual that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual
   a. This includes past, present or future payment for provision of health care
   b. This includes the fact of having an account with a vendor of PHRs or a related entity
   c. This does not include de-identified information as HIPAA defines it (NOTE: The FTC does consider the limited data set as defined by HIPAA as PHR identifiable health information)
6. PHR related entity –
   a. Entities that are not HIPAA covered entities that offer products or services through the website of a vendor of PHRs
   b. Entities that are not HIPAA covered entities that offer products or services through the websites of HIPAA covered entities that offer PHRs
   c. Non-HIPAA covered entities that access information in a PHR or that send information to a PHR – the main intent here is to reach those entities that provide online applications individuals may use for self reporting data to their PHR such as home glucose monitoring
7. Third Party Service Provider –
   a. An entity that provides services to a vendor of PHRs or a PHR related entity in connection with offering or maintaining a PHR
   b. An entity that accesses, maintains, modifies, records, stores, destroys or otherwise holds, uses of discloses unsecured PHR identifiable health information as a result of such services
8. 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 personal health information – this guidance issued by the Secretary on April 17, 2009, may be found at - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf
   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
9. Vendor of Personal Health Records – an entity other than a HIPAA covered entity or an entity that engages as a business associate of a HIPAA covered entity that offers or maintains a personal health record

Scope of Regulation

The FTC has regulatory authority over consumer related commercial interests where the interests cross state lines. That applies in the case of personal health records.

The rule applies to three types of entities. The rule directly regulates PHR vendors and PHR related parties which are defined above.. The rule also has requirements for third party service providers to play a similar role as a HIPAA Business Associate would play for a HIPAA Covered Entity. The rule does not apply to HIPAA Covered Entities or Business Associates. As a result, the rule does not apply to PHRs offered by HIPAA Covered Entities to their employees. Those kinds of PHRs would be covered by the breach
noticification requirements found within the breach notification rule that covers electronic health records issued by Health and Human Services (HHS).

The final rule focuses on breaches of “unsecured” individually identifiable PHI held in a PHR. 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 final regulation.

**Breach Notification Requirements**

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

**Timeliness of Notice**

1. Timely notification of the affected individual(s)
   a. A regulated entity must notify the affected PHR customers within 60 days of the day of discovery of the breach
      i. This applies to all notifications except for the notification to the FTC that the breach has occurred
         1. 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
         2. If additional affected customers 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 customers
      ii. The day of discovery will be considered the day that the regulated 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 regulated entity or a third party service provider working on behalf of the regulated entity becomes aware of the breach
         2. The regulated entity will be considered aware of a breach if any of its employees or agents is aware or reasonably should be aware of the breach
      iii. Third party service providers must provide notice to the regulated entity of any such breaches that they may become aware of
         1. Receipt of this notice must be acknowledged by a senior official of the regulated entity
         2. The notice shall contain an identification of each affected individual
   iv. The concept of “reasonably should have known” means that the FTC expects entities that collect and store unsecured PHR identifiable health information to maintain reasonable security measures including breach detection measures to assist in detecting breaches in a timely manner
      1. An entity 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 customers of the personal health record vendor or PHR related entity
   d. The notification requirement under the FTC rule does not apply to breaches involving PHRs offered by a HIPAA covered entity or business associate – the HHS breach notification rule applies in those cases
      i. PHR vendors or related entities that provide PHRs or related services directly to customers and to HIPAA covered entities who offer PHRs to their own employees, patients, enrollees, etc should maintain distinct lists of customers to
distinguish those who are their own customers and those who are using PHRs provided by HIPAA covered entities

1. This is so that the PHR vendor or related entity can separate out who they may have to provide direct notification to from who they would inform the HIPAA covered entity about that may be impacted by a breach

ii. Third party service providers can enter agreements with PHR vendors or related entities to provide notice to a designated senior official of the PHR vendor or related entity of breaches that the third party service provider becomes aware of

1. Third party service providers should obtain an acknowledgement of the receipt of such a notice from the senior official of the PHR vendor or related entity

2. The notice should be administered by

a. First class mail or by e-mail based on a customer’s meaningful choice as to the preference for receiving such notices considering what contact information is collected by the regulated entity

i. E-mail can be the default method for communicating the notice as long as the customer has the ability to make a meaningful choice regarding their preference

1. In the customer wishes to receive a notice by first class mail or other means, the regulated entity can indicate to the customer that additional personal information may need to be collected to accomplish the preferred method of notice

ii. Meaningful choice means that a customer is presented with their options for notification through a clear conspicuous means such as receiving an e-mail from the PHR vendor or related entity or through an alert upon access to their account

1. Such meaningful choice provisions cannot be buried in a Terms of Use type of document

2. The consent could be collected at the time of account creation with the PHR

b. Telephone or other appropriate means if there is possible imminent misuse of unsecured PHR identifiable health information

i. The regulated entity may institute processes to ask the customer for additional information to validate their identity if a phone based notification method such as a toll free number is used for customers to call into

c. Through other practical means of notice available to the PHR vendor or related entity if the primary means fails

d. In the case of failure to reach ten or more affected individuals, the regulated 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, bear appropriate wording if through a link on the web site, be available both on the home page for new users, and on the “landing” page for existing users

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. The FTC must also be noticed within 10 business days of any breach involving over 500 individuals

a. 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 the FTC 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
- Steps individuals should take to protect themselves from potential harm
  - 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 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 regulated 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

Reference

The final rule may be accessed at the following location –


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


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