Analysis of the Interim Final Rule, August 24, 2009
Breach Notification for Unsecured Protected Health Information

On Monday, August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule for breach notification in the case of unsecured protected health information, 45 CFR Parts 160 and 164, which are part of the Health Insurance Portability and Accountability Act of 1996. The regulations represented by this final interim rule (IFR) are a product of the American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII—Health Information Technology for Economic and Clinical Health (HITECH)—Subpart D on Privacy, signed on February 17, 2009.

NOTICE: ***This review of the Interim Final Rule: Breach Notification for Unsecured Protected Health Information is intended for an overview of the Rule and not as a definitive analysis. Readers seeking to comment on the IFR to the Department of Health and Human Services and those implementing the IFR are encouraged to read the entire Rule and not rely on this or any other summary of the Rule.***

The HITECH legislation prescribes a number of privacy components and a timetable for implementation, thus creating the timelines for compliance with these breach notification rules.

An electronic copy of this Interim Final Rule can be found on the electronic web pages of the *Federal Register* at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf, beginning on page 74FR42740. The Federal Trade Commission (FTC) has also issued a final rule on breach notifications for vendors of personal health records (PHRs) and similar non-HIPAA[1] entities. The FTC rule was published on August 25, 2009, and a separate analysis of that final rule will be published by AHIMA.

Author's Note: HITECH is a subset of the ARRA legislation (Title XIII). The Privacy sections—Subpart D—include Section 13402, which specifies the breach requirements included in HITECH. Therefore we will refer to HITECH and not reference ARRA as we review this IFR, unless there is a reference to a section of ARRA that is outside of HITECH.

The interim final rule for breach notification was not preceded by a notice of proposed rulemaking (NPRM); rather, the HHS Secretary published guidance on "Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" first on April 17, 2009 and then

[1] HIPAA refers to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

formally in the *Federal Register* on April 27, 2009. At that time the Secretary also requested comments related to the breach notification requirements as written in HITECH.

Note: AHIMA has instituted a webpage dedicated to items related to ARRA and HITECH legislation and regulation as well as items that can assist in the understanding and implementation of ARRA/HITECH. This webpage is located at www.ahima.org/arra.

Author's Note: Many of the terms used in the IFR refer to terms defined in HIPAA. The background section in the Preamble covers some of these terms, especially "protected health information (PHI)," which is a key term in the Rule. The HHS Office of Civil Rights (OCR) also provides examples of other terms identified in HIPAA Rules at 45CFR parts 160, 162, and 164. "Breach" is defined in HITECH, and HHS notes that it has modified that definition slightly. HHS also notes that HITECH defines "unsecured protected health information" which was further defined by the Secretary in the April 17, 2009 guidance (74FR19006 published on April 27, 2009).

Key Highlights of the Interim Final Breach Notification Rule

- **The effective date for this Rule is September 23, 2009.**
- **The full compliance date for this Rule is February 22, 2010.**
- **Because this is a Final Interim Rule, comments are requested by HHS as a new subpart D to part 164 of title 45 of the Code of Federal Regulations. As such covered entities need to understand the link between the new Rule and the previously issued Privacy Rule.**
- **This Rule becomes part of the HIPAA Rules.**
- **When a "breach" is discovered, HIPAA-covered entities and business associates have a maximum of 60 days to report (usually via the covered entity) the breach to the individual who is the subject of the breach, with some exceptions and variances.**
- **Covered entities will provide various reports to the Secretary including an annual report on all breaches that have occurred during a calendar year.**
- **Administrative requirements include workforce training, revision of business associate agreements, and the establishment of applicable policies and procedures.**

Key Dates for the HHS Breach Notification Interim Final Rule (IFR)

There are several key dates associated with this IFR:

- **Effective and compliance dates:**
  - The **effective date** for this IFR is **Wednesday, September 23, 2009**.
  - HHS is providing a grace period of sorts and indicates (74FR42757) that it will not expect **full compliance** until **Monday, February 22, 2010**.
  - The Rule affects all HIPAA-covered entities in addition to Business Associate as defined in Sections 13401, 13402, and 13404 of HITECH.

- **Comment due dates**—IFRs permit comments on the Rule. This particular IFR has two comment periods:
    - **Comments on the information collection requirements** associated with this IFR are due on or before **September 8, 2009.**
    - **Comments on the provisions** of this IFR are due on or before **October 23, 2009**.
    - In an IFR such comments could cause HHS to revise the Rule.
    - Instructions on where, what, and how to send comments are included in the IFR on the first page—74FR42740.
    - Specific questions can be directed to HHS—Andra Wickes at (202) 205-2292.
    - AHIMA will be making comments as appropriate.

The Interim Final Regulation for Breach Notification

The specific requirements for Breach Notification begin on page 74FR42767 of the August 24, 2009 *Federal Register* Rules and Regulations. The new IFR has been incorporated into the HIPAA regulations Parts 160—164. Accordingly, the new IFR has added a Part D and caused other sections of the HIPAA Rule to be modified.

Part 160—General Administrative Requirements (74FR42767)

The changes in Part 160 are mainly to incorporate the Breach Notification Rules in Part D of HIPAA Section 164 into the full Rule. This requires adding language to some sections, and revising or moving definitions so that they apply correctly.

- Section 160.101 of HIPAA, **Statutory Basis and Purpose**, is revised to reflect the HITECH statutes, Public Law 111-5, being added and to identify the authority for the added regulations.
- Section 160.101, **Statutory Basis and Purpose**, is also revised to identify the section of HITECH—namely Section 13402—as the source of the added regulations.
- Section 160.202, **Definitions**, revises the second paragraph of the definition of "Contrary." The definition of contrary now reads:
    - ***Contrary***, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means
        - "(1) A covered entity could find it impossible to comply with both the State and federal requirements; or
        - (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or section 13402 of Public Law 111-5, as applicable
- Section 160.534, **The [administrative law judge] Hearing**, has added a item (b) (1) (iv) indicating that the respondent in a hearing has the burden of going forward and the burden of persuasion with respect to any:
    - "Compliance with subpart D [breach notification] of part 164, as provided under 164.414 (b)."

- Section 160.534, **The Hearing**, also has a revision to (b) (2), which now reads:
    - The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

Part 164—Security and Privacy (74FR42767)

- Again the **Authority Citation** for this section is revised to incorporate Public Law 111-5.
- Section 164.102, **Statutory Basis,** is also revised to reflect Section 13402 of Public Law 111-5.
- Section 164.103, **Definitions**, adds in alphabetical order the definition of law enforcement official. This is referenced in the Rule that permits a delay in providing a breach notice at the request from such an official. The definition reads:
    - ***"Law enforcement official*** means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
        - (1) Investigate or conduct an official inquiry into a potential violation of law; or
        - (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law."
- Section 164.304, [Security Standards] **Definitions**, adds a definition:
    - ***"Access*** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."
    - **Author's Note:** this definition only applies to the section on Security, and not the sections on Breach Notification or Privacy.
- Finally, the IFR adds a new **subpart D to part 164,** which reads as follows:
    - Subpart D—Notification of the Case of Breach of Unsecured Protected Health Information
        - Section 164.400: Applicability
        - Section 164.402: Definitions
        - Section 164.404: Notification to individuals
        - Section 164.406: Notification to the media
        - Section 164.408: Notification to the Secretary
        - Section 164.410: Notification by a business associate
        - Section 164.412: Law enforcement delay
        - Section 164.414: Administrative requirements and burden of proof.

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information (74FR42767-70)

Applicability—Section 164.400

This section simply notes that the requirements of Subpart D apply with respect to breaches of protected health information occurring on or after September 23, 2009.

- **Author's Note:** While the effective date is September 23, 2009, HHS/OCR has indicated in the Preamble that it will provide a period until February 22, 2010, where it will "use our enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered…we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance."
- **Author's Note:** While a full compliance date appears not to take place until February 22, covered entities should review all breaches, provide a risk assessment, and definitely log the situation as required. Each covered entity will still be governed by state laws, and will have to determine why it should not notify affected parties in case of breach. The log of breaches that is required for reporting to the Secretary will cover the period of September 23 to December 31, 2009, for the 2009 reporting period.

Definitions—Section 164.402

Two new definitions are part of this subpart D. Other definitions used in the Rule generally refer to definitions previously developed in HIPAA. The two definitions, key to the new Rule, are:

- ***"Breach*** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E [Privacy] of this part which compromises the security or privacy of the protected health information.
    - (1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.
    - (ii) A use or disclosure of protected health information that does not include the identifiers listed at Section 164.514(e)(2) [Other Requirements—Standard Limited Data Sets—Implementation Specification], date of birth, and zip code does not compromise the security or privacy of the protected health information.
    - (2) Breach excludes
        - "(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a 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 under subpart E [Privacy] of this part.
        - (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized healthcare 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 subpart E [Privacy] of this part.
        - (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information."

- **Author's Note**: In the IFR, HHS made some minor adjustments to the breach definition in HITECH. The Preamble to this Rule also goes into some depth (74FR42743-45) in describing situations or circumstances that might fit the three exceptions. An assessment will need to be made by the covered entity or business associate to determine if the situation does not constitute a breach. It should be made clear in workforce training that this is an assessment the designated authority should make and employees should not take it upon themselves to make such a judgment and not report an incident to the designated authority. The Rule does not define an authority, however, since the IFR is now part of HIPAA and there is considerable overlap with the Privacy Rule. It would make sense to have the covered entity's privacy officer designated to initiate any action related to breach.

- ***"Unsecured protected health information*** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402 (h) (2) of Public Law 111-5 on the HHS Web Site."
  - **Author's Note:** As part of the Preamble to this IFR, HHS updates the guidance noted in this definition from that provided by the Secretary on April 17, 2009, and published in the *Federal Register* on April 27, 2009 (74FR19006). When HHS issued the April guidance on secure data, it asked for comments on the guidance technology and approach specified. The Preamble to this IFR (74FR42741) discusses these comments and essentially leaves the guidance as it stood in April. HHS is to provide annual guidance, and the guidance also applies to the FTC's Breach Notification Rules for non-HIPAA entities. HHS also notes, as commented on in the definition, that it will continue guidance publication on its Web site http://www.hhs.gov/ocr/privacy/.
  - **Author's Note:** In the Preamble HHS also goes into detail on a number of subjects including encryption requirements and definitions, NIST assistance, and other items related to unsecure information. Readers are urged to review this section, and further review is made in the Preamble comments below.

Notification to individuals—Section 164.404

The next several requirements are addressed in a manner similar to previous HIPAA sections. A standard is provided and then implementation specifications are listed.

Standard

- **General Rule:** A covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI "has been or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.
- **Breaches treated as discovered:**
  - For the purposes of notifying individuals or the media, a breach shall be treated as discovered as of the first day on which such breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity.
  - A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is a workforce member [HIPAA

definition] or "agent of the covered entity (determined in accordance with the federal common law of agency)."

- **Author's Note:** Workforce is a HIPAA concept and under HIPAA the entity is responsible for a much larger group than just its employees. HIPAA required the workforce to be trained and the requirement here implies that the workforce will be trained in what a potential breach is and what to do if they discover a potential breach has occurred. The implementation specification further addresses this as does the Preamble for this IFR.
- **Author's Note:** This is the first time the term "agent" enters this Rule. Agent does come up in the HIPAA Subpart on the Imposition of Civil Money Penalties. Whether the discovery of a breach is by a member of the workforce, a business associate, or an agent will be receiving some additional attention with regard to timing and will be discussed further below.

Implementation Specification

- **Timeliness of notification:** except when there is an appropriate law enforcement delay, a covered entity shall provide the notification required without reasonable delay and in no case later than 60 calendar days after discovery of a breach.
  - **Author's Note:** 60 calendar days is the maximum (ignoring the agency question), however, HHS notes several times in the Preamble that there are a number of reasons why notification should be sooner than 60 days, either because of state law which is not preempted, possible harm to the individual, or because there is no reason to delay based on the facts at hand. Covered entities should be careful in writing their breach policies and procedures not to suggest that notification will not occur until after 60 days. It should also be noted that organizations that have experienced breaches often come under public scrutiny, and taking a full 60 days could cause the entity problems from a public relations standpoint. On the other hand, risk assessments should not be unduly rushed and cause an inappropriate result. The law enforcement delay will be addressed in a later section.
- **Content of notification:**
  - **Elements:**
    - 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 PHI** that were involved in the breach.
    - Any **steps individuals should take** to protect themselves from potential harm resulting from the breach.
    - A brief description of **what the covered entity involved is doing** to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
    - **Contact procedures** for individuals to ask questions, or learn additional information, including a toll-free telephone number, an e-mail address, Web site, or postal address.
  - **Plain language requirement—**the notification shall be written in plain language.
  - **Author's Note**: The Preamble discussion (74FR42750) provides further descriptions of the elements of the notice and alternatives a covered entity should consider.

- **Methods of individual notification** provide the form for notification and substitute notices to use in certain circumstances.
    - **Written notice:**
        - The notice must be by first-class mail to the last known address of the individual or their representative, or
        - The notice can be sent by electronic notice if that has been the agreed-upon form of notice between the entity and the individual and this agreement has not been withdrawn.
        - The notification may be provided in one or more mailings as information is available.
        - If the individual is deceased then the notice following the same rules must be sent to the next of kin or personal representative as specified in the Privacy Rule.
    - **Substitute notice:**
        - If the written notice cannot be received due to insufficient or out-of-date contact information, then the covered entity must consider a substitute form of notice calculated to reach the individual. However, if the individual is deceased and the next of kin or personal representative cannot be contacted, no additional steps need to be taken with a substitute notice.
        - The substitution notice varies depending on the number of individuals affected by the breach:
            - If less than 10 individuals are involved the substitute notice can be by phone or other means.
            - If 10 or more individuals are involved, the substitute notice shall:
                - Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved *or* a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside, *and*
                - Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHR may be included in the breach.
        - **Author's note:** This is a fairly detailed specification; however, once again HHS has provided even more detail in the Preamble including how a substitute notice should be posted on the covered entities Web site and what constitutes choosing media in a geographic area. While the detail in the Preamble is not a requirement, covered entities would do well to heed the advice since any follow-up by the OCR will most likely include questions as to whether this advice was known and followed.
    - **Additional notice in urgent situations—**if the covered entity determines that the breach situation is urgent because of possible imminent misuse of unsecured PHI, it may provide information to individuals by telephone or other means, as appropriate. However, this does not eliminate the need for the required written notice.

Notification to the media—Section 164.406

Standard

- For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. States include American Samoa and the Northern Mariana Islands.
    - **Author's Note:** in the Preamble (74FR42753) HHS clarifies that "State" is defined by HIPAA [Section 160.103], and therefore not spelled out in this Rule. The two territories named, however, were not in the HIPAA definition. HHS also clarifies that "**jurisdiction**" is a geographic area smaller than a state, such as a county, city, or town.
    - **Author's Note:** The clarification just given is important because, as HHS provides by example in the Preamble, if the number of individuals is greater than 500, but multiple states are involved and no one state has 500, it is possible that no notification is necessary.

Implementation Specifications

- **Timeliness of notification**—again, except for law enforcement delays, the notification to the media must come without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- **Content of notification**—the notification to the media in this case must meet the same requirements as the notice to individuals.
    - **Author's Note**: in HHS' discussion in the Preamble (74FR42753) it is suggested that HHS "expect[s] that most covered entities will provide notification to the media under this section in the form of a press release."

Notification to the Secretary—Section 164.408

Standard

- A covered entity shall, following the discovery of a breach of unsecured protected health information, notify the Secretary.

Implementation Specifications

- **Breaches involving 500 or more individuals**—requires the covered entity, with an exception for law enforcement delays, provide notice "contemporaneously" with the notice to the individual and in a manner specified on the HHS Web site.
- Breaches involving less than 500 individuals—requires a covered entity maintain a log or "other documentation" of such breaches and, not later than 60 days after the end of the calendar year, provide the notification required for breaches occurring during the preceding calendar year, in a manner specified on the HHS Web site.
    - **Author's Note**: At the initial writing of this analysis nothing had been posted by HHS on the web site. We presume instructions will be forthcoming by the September 23, 2009 date since the date for the submission of a log of CY2009 breaches (September 23—December 31, 2009) will be March 1, 2010, which occurs after the compliance date indicated by HHS. While the implementation specification does not

indicate, we suspect that all determined breaches should be listed including those that might be reported under the greater than 500 instruction.

Notification by a business associate—Section 164.410

Standard

- A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.
- A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

Implementation Specifications

- **Timeliness of notification**—with the exception for a law enforcement delay, a business associate is required to provide notification as required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
    - **Author's Note**: The **timeliness** of notifications must become a subject of contract or business associate agreement between the covered entity and the business associate. Both have a 60-day period, but, conceivably, if the business associate does not turn the necessary information over to the covered entity, the covered entity's ability to meet its obligations to the individual and be compliant with this Rule could be in danger, if the business associate is functioning as an agent of the covered entity, rather than as an independent contractor. It will be prudent for covered entities to work out how each party will handle breaches, and of course this arrangement could vary with each business associate of the covered entity and the type of work being done by the business associate. The Rule's Preamble discussion also suggest that there may be times when it is appropriate for the business associate to take the lead in notifying the individual since the business associate may be more familiar with the situation than is the covered entity.
    - **Author's Note**: The Rule and the Preamble (74FR42754) also raise the question of "agency," a concept first introduced in the HIPAA Enforcement Rule. Under certain circumstances the various relationships will have an impact on the responsibilities of the parties and the issue of timeliness. It is conceivable, according to the Preamble and our contact with OCR, that in the case of an independent contractor, the clock for timeliness on the part of the covered entity will not start until the independent contractor informs the covered entity of the breach. Taken at the full contingency, this could mean a period of 120 days could pass before the individual would have to be notified. While some may see this as preferable, others would suggest that the reputation of the covered entity and perhaps the business associate would suffer from a delay of many months, whether or not the Rule permits such a delay. Readers are urged to review the Preamble discussion and consult with their attorney. Again there is nothing in these situations that would prevent the covered entity and its related parties from setting up timelines of less duration than that permitted by the Rule.

- **Author's Note**: A breach at a business associate raises a situation where if a personal health record is involved; the covered entity will have to consider the business associate's status relative to the FTC Rules on Breach Notification. When there is overlap, the HHS Rule prevails, and any notification under it will suffice for any FTC audit or investigation.

- **Content of notification**
  - The required notification shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used, or disclosed during the breach.
  - The business associate shall provide the covered entity with other available information that the covered entity is required to provide in its notification to the individual within those timelines and any additional information as it becomes available.
  - **Author's Note:** The Rule's Preamble suggests scenarios where the amount of information available at the business associate may be limited because of the nature of the associate's activities. Again, this should dictate any agreement between the two parties, but also what may be necessary to do a risk assessment of the situation. The Preamble also suggests that a business associate could have a breach of PHI that affects more than one covered entity. Such a situation could have other ramifications that would have to be considered including consultation among the covered entities.

Law enforcement delay—Section 164.412

HHS has recognized that there may be situations where notification of the individual or media could impact a criminal investigation. This section requires that if a law enforcement official (defined above) states to a covered entity or business associate that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, then the covered entity or business shall:

- (a) When the **statement is in writing and specifies the time** for which a delay is required, delay notification, notice, or posting for the time period specified by the official; or
- (b) When the **statement is oral,** document the statement including the identity of the official making the statement and delay the notification, notice, or posting temporarily, but no longer than 30 days from the date of the oral statement, unless a written statement (a) is received within the required time period.
- **Author's Note:** It must be noted that the entire law enforcement delay may occur within the 60-day time period allotted to the covered entity or the business associate. The IFR does not provide for a delay in the risk assessment or other activities required or suggested in the IFR. One might presume that an official investigation affirms both the breach and the potential harm to the individual, but it is possible more information on this requirement will be forthcoming from the OCR.

Administrative requirements and burden of proof—Section 164.414

This section refers to the HIPAA Privacy subpart E and parts of its Section 164.530, Administrative requirements.

- **Administrative requirements**—a covered entity is required to comply with the administrative requirements of the HIPAA Privacy Rule (and further amended in a revised Section 164.530 below) related to:
    - Training,
    - Complaints to the covered entity,
    - Sanctions,
    - Refraining from intimidating or retaliatory acts,
    - Waiver of rights,
    - Policies and procedures, and
    - Documentation.
- **Burden of Proof**—in the event of a use or disclosure in violation of the Breach Notification subpart—now part of HIPAA—the covered entity or business associate as applicable, shall have the burden of demonstrating that all notifications were made as required or the disclosure did not constitute a breach as defined.

Amended—Section 164.501

- This section amends several sections of the HIPAA Privacy Rule to allow conformance with the inclusion of the new Breach Notification IFR.
- Significant amendments are made to **HIPAA Section 164.530 [Administrative requirements]** and those changes are highlighted (underlined) below.
    - (b) (1) ***Standard Training: Training***. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D [Breach Notification] of this part as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.
    - (b) (2) ***Implementation specifications: Training***.
        - (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
            - (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
            - (B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
            - (C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D [Breach Notification] within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
            - (C) (ii) a covered entity must document that the training described in paragraph (b) (2) (i) of this section has been provided, as required by paragraph (j) of this section.
    - **(d) (1) *Standard: Complaints to the covered entity.*** A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D [Breach Notification] of this

part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

- (d) (2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received and their disposition, if any.
- **(e)(1)** ***Standard: Sanctions*** A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D [Breach Notification] of this part.
- (e) (2) *Implementation specification: documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.
- **(g)** ***Standard: Refraining from intimidating or retaliatory acts.***
  - (1) May not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D [Breach Notification] of this part, including the filing of a complaint under this section; and
  - (2) Must refrain from intimidation and retaliation as provided in §160.316 of this subchapter.
- **(h)** ***Standard: Waiver of rights*****.** A covered entity may not require individuals to waive their right under §160.306 [Complaints to the Secretary] of this subchapter, this subpart, or subpart D [Breach Notification] of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- **(i) (1)** ***Standard: Policies and Procedures***. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D [Breach Notification] of this part;
- **(i) (2)** ***Standard: Changes to Policies and Procedures.***
  - **(i)** A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements and implementation specifications of this subpart or subpart D [Breach Notification] of this part.
  - (ii) When a covered entity changes a privacy practice that is stated in the notice described in §164.520 [Notice of privacy practices for PHI], and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that is created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with §164.520, included in the notice a statement reserving its right to make such a change in its privacy practices; or
  - (iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i) (5) of this section.
- (i) (3) *Implementation specification: Changes in law*—No Change
- (i) (4) *Implementation specifications: Changes to privacy practices stated in the notice.*—No Change

- (i) (5) *Implementation specification: Changes to other policies or procedures.*—No Change.
- **(j)** A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D [Breach Notification] of this part.
- **(**j) (1) *Standard: Documentation.* A covered entity must:
  - (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;
  - (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation;
  - (iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation; and
  - **(iv)** Maintain documentation sufficient to meet its burden of proof under §164.414 (b) [Burden of proof].
- (j) (2) *Implementation specification: Retention.*—No Change.

- **Author's Note**: While this section merely updates HIPAA §164.530 [Administrative Requirements] it essentially requires new training of the workforce as well as new or revised policies and procedures. These changes need to be made in the next six months before the compliance date; however, key personnel should be advised immediately and brought up to speed on this IFR requirement. We expect that there will be considerable publicity at the time these rules become effective in September 2009, and there will be public expectations even if the OCR has moved a final compliance date back to February. Covered entities should be prepared to discuss these Rules with the public and the press as early as possible.

Preamble to the Breach Notification

Preambles are written for most final or interim rules to provide the background for the rule as it is presented. As we have noted several times above IFR's Preamble does an excellent job in providing HHS' thinking on the various sections for the Breach Notification IFR as well as providing suggestions and examples on how a covered entity or business associate respond to a breach and carry through the requirements of the Rule.
Generally, in its Preambles, HHS will first state grouped comments to its proposed rules, respond to these comments, and finally provide the rational for the regulation as finally written. This IFR is different since there was no notice of proposed rulemaking. HHS did invite comments on the pending regulation attached to its April guidance on unsecure protected health information. These comments were made with only the HITECH legislation at hand and HHS provided limited information as to what it would propose in a rule. Accordingly, in this IFR Preamble HHS and OCR take the tact to essentially follow the legislation, address the comments received, and then provide the rational for the rule being presented. The preamble is approximately 26 pages and for maximum compliance well worth the time to review.

I. Background (74FR42740-41)

The background section for this IFR is relatively simple. It references ARRA and HITECH legislation passed in February 2009 that served as the impetus for this Rule, as well as the Health

Insurance Portability and Accountability Act of 1996, PL104-191(HIPAA), which is referenced quite often in the regulation itself. HHS notes that these rules or regulations apply to HIPAA entities defined by that Act and subsequent regulations. Finally, the Background section provides a very general overview of the rule or regulation (terms often used interchangeably) as was noted above and further commented on below.

II. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74FR42741-43)

HHS provides background specifically on the security guidance called for by HITECH. HITECH was clear that if health information were "secure" then a breach could not occur. Only when protected health information is not secure can a 'breach" occur. HITECH called on the Secretary to provide ongoing guidance as to what technologies could be deemed to provide such protection, and this was the subject of the Secretary's April guidance. It should be noted that the Secretary's guidance also applies to breach rules for non-HIPAA entities, mainly personal health record (PHR) operators and their third parties who are covered by a rule issued on August 25 by the FTC.

The definition of protected PHI is repeated in this IFR both to reiterate the role of the guidance on determining breach, and to address comments made by the industry and public on the April guidance. The technologies for approved protection must render the PHR "unusable, unreadable, or indecipherable to unauthorized individuals." The April guidance identified encryption and destruction as the technologies and methodologies for rendering PHI secure.

Several questions were raised as to whether the Secretary's guidance now made the use of encryption a standard under the HIPAA Security Rule. HHS indicates that this is not the case and there may be legitimate reasons for an entity not to choose encryption and still be compliant with the Security Rule. HHS, however, notes that should a breach occur, there is the possibility that the entity could be subject to the breach notifications requirements in this IFR. HHS comments are a reminder that HIPAA-covered entities and Business Associates, who became subject to some of the HIPAA security Rule as identified in HITECH Section 13401, must work together in addressing breach situations.

In response to inquiries, HHS clarifies the forms of information addressed in the National Institute of Standards and Technology (NIST) publications and referenced in the guidance. HHS clarifies these forms as:

- Data in motion—data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange;
- Data at rest—data that resides in databases, file systems, flash drives, memory, and any other structured storage method;
- Data in use—data in the process of being created, retrieved, updated, or deleted; and
- Data disposed—discarded paper records or recycled electronic media.

In response to the suggestion that "access controls" be included in the guidance protections, HHS acknowledges and supports the role of access controls in making breach less likely, but indicates that they do not prohibit a breach from occurring.

HHS provides a discussion on redaction and the use of "limited data sets" (74FR42742 and 32745) and when they might serve to eliminate a possible breach in both satisfying HIPAA Section 164.514, and the issues of "harm." HHS makes the case that information that is successfully redacted to meet the HIPAA definition of a limited data set and has taken into consideration two additional date elements—birth date and zip code—then there is the potential that the data would no longer defined as protected health information and harm is mitigated; therefore creating a situation where the incident is not subject to the breach notification requirements. These sections, as well as the original HIPAA Rule, require careful reading.

With regard to using encryption, HHS notes that for the purposes of its new guidance (concurrent with this IFR) there are two additional clarifications regarding encryption, namely:

- To ensure encryption keys are not breached, covered entities and business associates should keep encryption keys on a separate device from the device that carries the data they encrypt or decrypt.
- To provide additional guidance with regard to NIST, a roadmap on guidance activities on the part of NIST pertaining to data storage on enterprise-level storage devices such as RAID (redundant array of inexpensive disks) or SAN (storage-attached network) systems. The NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to the guidance, when available.

Author's Note: It appears when reviewing these comments that, currently, many smaller entities subject to the guidance may not be prepared technically to use the technologies identified by HHS for securing PHI at this time. Hopefully, this will change over time as new technologies can be defined.

Finally this guidance section, as part of the IFR, serves as the updated guidance as of August 24, 2009, noting (74FR42742) that PHI is "rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:"

- Electronic PHI has been encrypted as specified in the HIPAA Security Rule and following specified NIST publications, or
- The media on which the PHI is stored or recorded have been destroyed in a specified manner.

III. Overview of the Interim Final Rule (74FR42743)

HHS begins the overview of the IFR by noting the newly created a subpart D to part 164 of title 45 of the Code of Federal Regulations. This put the new regulations into the HIPAA Rule and resulted in HHS moving several of the definitions used within HIPAA.

HHS provides a description of its actions with the FTC so that the breach notification rules of both are consistent, and the entities covered by each understand which rule must be complied with. HHS notes that concerns were raised that individuals might receive more than one notice as

a result of overlap between HHS and the FTC. The harmonization of the rules between the two federal bodies should result in both rules being complied with by the same letter.

IV. Section-Section Description of Interim Final Rule (74FR42743)

The Overview proceeds through each section of the new Rule. We are highlighting here those items in the Overview that might provide clarification to the reader beyond our comments above.

Applicability (Section 164.401)

This section just notes that the IFR is effective in 30 days from publication in the *Federal Register*—September 23, 2009.

Definitions (Section 164.402)

HHS provides the background on how definitions were adopted especially if the definition has any deviance from that in HITECH.

Breach

- **Breach**—the definition of breach in the new Rule reads: "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [requirements in the IFR] which compromises the security or privacy of the protected health information." The definition then is followed by defining when security is considered compromised and exceptions. Note that the key here is PHI. If PHI is not involved there is no breach as far as this federal rule goes.
    - HHS defines "unauthorized" as the "impermissible use or disclosure of PHI under the HIPAA Privacy Rule."
    - HHS notes that not all violations of the Privacy Rule are necessarily breaches as defined in this IFR. Therefore, an impermissible use and disclosure under Privacy might not be a breach.
    - HHS further notes that not all violations of the Security Rule would be considered a breach, but they could be a violation of the Privacy Rule.
    - While HHS was asked by some to define "acquisition" and "access," the Department believes these are common definitions and chooses not to define them further.
    - HHS then provides a lengthy discussion of the overlap of the Privacy, Security, and Breach Notification Rules. Readers preparing compliance plans and training should read this section of the Overview (74FR42743-44).

- **Compromise the Security or Privacy of Protected Health Information**—rather than an initial definition, HHS continues the discussion on the overlap of the three rules—Privacy, Security, and Breach Notification—and what steps an entity should take to determine the nature of the incident. HHS raises the issue of **harm** in this discussion and, based on comments and a review of state laws related to breach, suggests that there is a harm threshold that should be cited in the Rule. Therefore, HHS has agreed that the statutory language encompasses a harm threshold and therefore is clarifying the "compromise" definition that

harm means the breach or compromise "poses a significant risk of financial, reputational, or other harm to the individual."

- This discussion leads to suggest that "to determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities, and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure." The discussion (74FR42744-46) then provides factors to consider related to determining harm and how covered entities should go about the performance of a risk assessment, including what documentation should take place.
- The issue of "limited data sets" is further discussed in this section. HHS suggests that a risk assessment be done with regard to a breach of what may have been a limited data set.
- **Author's note:** Since this is a IFR with comment, we expect to see a further discussion of "harm" in the months to come, and it is possible that clarification will continue in any amendment to the Rule.

- **Exceptions to Breach**—HHS notes that Section 13400(1) of HITECH provides exceptions to the definition of "breach," essentially under certain circumstances these include
  - Unintentional acquisition, access, or use of PHI,
  - Inadvertent disclosure of PHI among "authorized" individuals , and
  - Disclosure in situations where the unauthorized individual could not be expected to retain the information.

  The discussion goes into detail for each of these exceptions and examples are provided to describe the relationships of persons to the covered entity, business associate, or enterprise, as well as the disposition of the breached PHI when an act on the part of person or persons occurs. This is required reading (74FR42746-48).

Unsecured Protected Health Information

- This section describes PHI and its relationship to the definition in HITECH and the Guidance provided by the Secretary (and updated in this Preamble).
  - Unsecured Protected Health Information is defined for the IFR as: "…protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance."
  - The Preamble points out that further guidance from the Secretary will be available on the HHS Web site at http://www.hhs.gov/ocr/privacy. If the reader has not signed up to be notified when this site is updated, please consider it.

Notification of Individuals (Section 164.404)

This section of the Preamble covers the issues of the general rule, discovery, timeliness, content, methods of notification, and additional notice in urgent situations. These issues were covered in some detail above and the reader is urged to review this discussion (74FR42748-52). Briefly the discussions include:

- **General Rule** (74FR42749): Here the Preamble discusses a few of the changes that were made between HITECH and the IFR.
- **Breaches Treated as Discovered** (74FR42749): This discussion covered when discovery occurs and by whom (someone other than the person committing the breach) as well as the reasonableness of the covered entities actions. The discussion continues to cover the actions and timeliness of actions of the covered entity or business associate including reasonable diligence.
- **Timeliness** (74FR42749-50): This section covers when certain actions should take place. It is suggested that reasonable time be given to the risk assessment process; however, it is also noted that the covered entity can provide multiple notices to the affected individual, so the entity must balance the individual's right to know with the potential harm that could be inflicted, and the status of the risk assessment. This section also addresses comments as to the period selected for maximum response—60 days. This section further addresses time requirements from State or other laws.
- **Content** (74FR42750): The content discussion covers the points in the Rule and what detail might be provided under each to give the individual (and the entity) the ability to mitigate harm. HHS notes that covered entities must be careful not to disclose further PHI in the process by providing the exact information/data that was discussed.
- **Methods of Notification** (74FR42750-52): This is an extensive section since there are multiple ways an entity may use to notify an individual depending on the ability to find the individual or next of kin. It is also affected by the numbers of individual that may be affected by the breach. The method of notification will affect the content of the notice. This section provides a number of alternatives for covered entities to consider.
- **Additional Notice** (74FR42752): This very short section notes that in an urgent situation a notice can be phoned to prevent harm to the individual. A phone call does not eliminate the requirement for a written notice.

Notification to the Media (Section164.406)

This section on Media (74FR42752-53) covers a number of issues in detail including:

- The use of notification through the media as an alternative method of notice for situations affecting 500 or less individuals, versus the notification requirement when a breach has affected more than 500 individuals. In the case of the former, HHS indicates its belief that the notice to the media could be in the form of a press release.
- The Rule calls for "prominent media" but does not define "prominent" here; rather it suggests how an organization would determine prominent media depending on location of the covered entity and affected individuals.
- HHS also notes when the media must be utilized depending on the number of individuals making up the more than 500 quota, when multiple "States" might be involved.
- This section also covers some of the content that must be provided by the covered entity.

Notification to the Secretary (Section 164.408)

The discussion in this section (74FR42753) lays out detail and timing related to the two different notifications the covered entity might use in contacting the Secretary, depending on the number

of individuals involved in the breach. Key details are spelled out in the IFR, and additional detail is to be provided on the HHS Web site.

Notification by a Business Associate (Section 164.410)

This is a rather long section (74FR42753-55) covering not only the obligations of the business associate, but also the manner in which notification must take place. As noted in our review of the IFR (above), the issue of **Agency** is raised in Section 164.410 and a limited discussion takes place here with reference to the HIPAA Enforcement Rule. The issue is, when does the clock start for the covered entity—when the discovery occurs at the business associate or when the business associate first contacts the covered entity? The common law of Agency differentiates between an "agent" and an "independent contractor," and HHS does not provide a clear distinction here, leaving it up to the covered entity and associate to determine.

- **Author's Note**: As noted above, covered entities can clear up the ambiguities raised here in their contracts, but covered entities must also understand that even though HHS has raised the potential for a period of notification to extend beyond 60 days, the public or media might not accept such an extension. In either case, harm to the individual should dictate how immediate a response is reasonable, and we expect HHS will be reasonable in any follow-through to a breach situation.

This section also covers the potential for overlap between the HHS **and FTC Breach Notification** rules and notes in "those limited circumstances where a vendor of PHRs (1) provides notice to individuals on behalf of a HIPAA-covered entity, (2) has dealt directly with the individuals in managing their PHR accounts, and (3) provides notices to its [other] customers at the same time, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be in compliance with the corresponding FTC rule provisions."

Law Enforcement Delay (Section 164.412)

This rather short section (74FR42755) simply provides a more detailed description of the statement needed to permit a law enforcement delay.

Administrative Requirements and Burden of Proof (Section 164.414)

Essentially this short (74FR42755) section ties together the new IFR rules for administrative requirements and burden of proof with those already in existence under the HIPAA Privacy Rule.

Other Conforming Changes to the HIPAA Rules

Similar to the previous section this section merely covers other conformance changes.

Preemption

This section (74FR42756) responds to comments and questions related to preemption and the new IFR. Preemption is already addressed in the HIPAA Rules and HITECH did not choose to change the preemption requirements for this new Rule. HHS notes that preemption is "implemented by 45 CFR 160.230 [HIPAA General Rule and exceptions], which states that a standard requirement or implementation specification that is adopted as regulation at 45 CFR parts 160 162, 164 and that is 'contrary to a provision of State law preempts the provision of State law.' Section 160.203 provides several exemptions in which State law will not be preempted; however, we do not believe these exceptions apply to the breach notification regulations…Therefore, contrary State law will be preempted by these breach notification regulations." HHS goes on to solicit comment in this area.

The section goes on to discuss the term "contrary," and notes that it has changed the definition of "contrary," mainly to include this Rule in the HIPAA definition. HHS suggests that covered entities will need to analyze relevant State laws with respect to this regulation to understand the interaction and apply this preemption standard appropriately. HHS goes on to provide some examples on how State law and this Rule might be compared.

Effective/Compliance Date

This section (74FR42756) covers the determination of the effective date and HHS' decision to extend the compliance period to February 22, 2010. HHS says that "during this initial time period—after this Rule has taken effect but before we are imposing sanctions—we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance."

V. Impact Statement and Other Required Analyses

Impact statements are required for all rules and an IFR is no exception. This review will be cursory given the nature of this IFR.

Introduction

The introduction covers the reasons for the impact statement and the various Acts and Executive Orders that require an impact review.

Why Is This Rule Needed?

HHS notes that the Rule is meant to respond to Section 13402 of the HITECH statute. HHS goes on to note the reasons behind this HITECH statute and the impact of breach on the individual. HHS also notes that there are costs behind breach reporting and suggests that some entities would not undertake such an activity unless required by law and regulation.

Costs and Benefits

In this section HHS lays out a summary of costs and benefits. HHS believes this will amount to some $17 million dollars based on its assumption of the number of breaches, methods of notification and reporting costs to HHS. HHS then breaks the cost down by the number of entities and breaches, and goes into more detail on defining what is a breach. It also provides some history on breaches and suggests that there were almost 2.9 million individuals affected by breaches as defined in 2008. Costs are also provided by the amount of first-class mail that is needed and alternative notifications. HHS also suggests costs for investigation of breaches and other administrative costs. The benefits of the Rule are also discussed in this section, including mitigation of financial loss and other impacts on the individual and covered entities.

Author's Note: Some privacy experts suggest that the numbers of breaches used in this analysis may be conservative, given data from some of the states, such as California, in 2009. This may be true; on the other hand, we are not quite sure if the reported breaches would have met the definition of a breach as specified in this Rule.

Regulatory Flexibility Analysis

The Regulatory Flexibility Analysis requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities, which is usually the case when healthcare providers are involved in a regulation. HHS submits that based on its analysis of data breaches for 2008 it does not expect the interim final rule to have a significant impact on a substantial number of small entities. HHS estimates that the average cost per breach will cost $160,616. Secondly, HHS suggests that the Rule will apply to entities that in many cases already have an obligation to provide notification under State law.

VI. Paperwork Reduction Act Information Collection

This section is also required by law and in response, HHS estimates that the total burden of hours annually will be 95,002 hours associated with notice to the individual, media, and the secretary.

MORE TO COME

With a comment period and future announcements already on the docket for this Rule, the reader should expect more to come and be prepared by signing up for the OCR Web site announcements mentioned above. Watch AHIMA's e-Alert and ARRA Web site for further information.