Analysis of the Final Rule, August 25, 2009
Health Breach Notification

On Tuesday, August 25, 2009, the Federal Trade Commission (FTC or the Commission) published a final rule, 16 CFR Part 318, for consumer breach notification for vendors of personal health records (PHR) and related entities in situations where the security of their individually identifiable health information has been breached. The regulations represented by this final rule 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. This Rule does not apply to HIPAA-covered entities.

NOTICE: ***This review of the Final Rule: Health Breach Notification is intended as an overview of the rule and not as a complete detailed analysis of the rule. Readers seeking to comply with this rule are encouraged to read the entire Final Rule and not rely on this or any other summary of the rule. In writing this Rule, the FTC presumes that readers are familiar with the notice of proposed rulemaking (NPRM) issued on April 20, 2009.***

An electronic copy of this Final Rule can be found on the electronic Web pages of the *Federal Register* at http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf, beginning on page 74FR42962. The NPRM preceding this rule can be found at http://edocket.access.gpo.gov/2009/pdf/E9-8882.pdf. The Department of Health and Human Services (HHS) has issued an interim final rule on breach notifications for unsecured protected health information for HIPAA-covered entities and business associates. The HHS rule was published on August 24, 2009, and a separate analysis of that final rule has been published by AHIMA.

Author's Note: HITECH is a subset of the ARRA legislation (Title XIII), and contains Privacy—Subpart D, including Section 13407 "Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities." We will refer to HITECH and not reference ARRA as we review this final rule, unless there is a reference to a section of ARRA that is outside of HITECH.

The Final Rule for Health Breach Notification was preceded by a proposed rule published in the *Federal Register* on Monday, April 20, 2009. AHIMA responded to this proposed rule and AHIMA's May 29, 2009 response can be found at the AHIMA Advocacy and Policy Web site www.ahima.org/dc/CommentsTestimony.asp.

Note: AHIMA has instituted a Web page 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 Web page is located at www.ahima.org/arra.

Key Highlights of the FTC Final Health Breach Notification Rule

- **The effective date for this Rule is September 24, 2009.**
- **The full compliance date for this Rule is February 22, 2010.**
- **The rule covers, personal health record (PHR) entities not subject to HIPAA including:**
  - **Vendors of personal health records;**
  - **PHR-related entities; and**
  - **Third-party service providers.**
- **When a "breach" is discovered these PHR entities have a maximum of 60 days to notify the individual related to the breached PHR information.**
- **Notification must take place using first class mail; however, there is an exception for an e-mail notification.**
- **When a "breach" is discovered and involves 500 or more individuals, the FTC must be notified within 10 days.**

Key Dates for the FTC Health Breach Notification Final Rule

There are two key dates associated with this Final Rule:

- **Effective and compliance dates:**
  - The **effective date** for this rule is **Thursday, September 24, 2009**.
  - **Full compliance** is required by February 22, 2010.

Further Information Contact

The FTC indicates that Cora Tung Han or Maneesha Mithal, attorneys in the Division of Privacy and Identity Protection can be contacted for further information on the Final Rule. Both attorneys are with the Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580 (202) 325-2252.

The Final Regulation for Health Breach Notification

The specific requirements for the Health Breach Notification Rule begin on page 74FR42962 of the August 25, 2009 *Federal Register* Rules and Regulations. The new Rule becomes Part 318 of 16 CFR and was required under Section 13407 of HITECH: Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities.

Author's Note: HITECH Section 13407 goes beyond the requirements for Breach Notification and establishes a number of joint efforts related to breaches and breach notification between the

FTC and HHS. Congress has indicated a sunset provision for these HITECH-based regulations should it enact new legislation establishing requirements for notification that would cover all entities HIPAA and non-HIPAA. HITECH also requires some reporting and recommendations from the FTC and HHS. These reports and recommendations could lead to such a change.

16 CFR Part 318—Health Breach Notification Rule (74FR42980)

This initial section establishes the new Rule. There is no reference to other sections as we have seen in HHS rules. The authority is established as Public Law 111-5, Statute 115 (2009) The sections for the Rule include:

- 318.1 Purpose and scope
- 318.2 Definitions
- 318.3 Breach notification requirement
- 318.4 Timeliness of notification
- 318.5 Method of notice
- 318.6 Content of notice
- 318.7 Enforcement
- 318.8 Effective date
- 318.9 Sunset

Purpose and Scope—Section 318.1 (74FR42980)

This section has two parts:

- Part (a) establishes the title "Health Breach Notification Rule," notes that it implements Section 13407 of HITECH, and applies to foreign and domestic vendors of personal health records (PHR), PHR-related entities, and third-party services providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizen or residents. The Part further describes that it does not apply to HIPAA-covered entities or business associates of HIPAA-covered entities.
    - **Author's Note:** Both the Preamble to this Rule and the Preamble to the HHS Interim Final Rule for Breach Notification describe situations where the relationship between a HIPAA-covered entity and a business partner might result in an overlap between the HHS and FTC rules. Accordingly, the rules have been coordinated so that a notification from a HIPAA–covered entity or business associate could serve the requirements of this Rule as well.
    - **Author's Note:** The Preamble (74FR42963-66) to this rule goes into a very long discussion on the scope of the FTC relative to this Rule and the overlap with HIPAA-covered entities and business associates. Entities concerned with their relationship to the FTC or HIPAA, or how this Rule fits in with the FTC as a whole will find this discussion of interest.
- Part (b) notes that this Part preempts state law as established in Section 13421 of the HITECH Part 2—"Relationships to Other Law…" which essentially set up this Rule similar to HIPAA preemption such that when the federal (FTC) rule is contrary to a state law the federal law will prevail.

Definitions—Section 318.2

Since this is a new Rule within the FTC, and the Rule in not a part of the HIPAA Rule, a number of definitions are listed so they may apply to this FTC Rule and be consistent with the new HHS Breach Notification Rule. Unlike the HHS HIPAA-based Rule, there is no mention of "protected health information" in this Rule

- (a) ***Breach of security*** means, with respect to unsecured PHR-identifiable health information of an individual in a PHR, acquisition of such information 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, PHR-related entity, or third-party service provider that experienced the breach has reliable evidence showing that there wasn't, or could not reasonably have been, unauthorized acquisition of such information.
    - Author's Note: The approach in the FTC Rule is different than that of HHS. The FTC has fewer exceptions to providing a notification and the Preamble of this Rule does not even consider provision for a risk assessment process.
- (b) ***Business associate*** is the definition provided by HIPAA 45 CFR 160.103.
- (c) ***HIPAA-covered entity*** is the definition provided by HIPAA 45 CFR 160.103.
- (d) ***Personal health record*** [in this Rule] means 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.
    - **Author's Note:** This definition limits PHR to "electronic" records; however, there is no description of *electronic*, which leaves a variety of digital-based products open for compliance, until a further description is given. The Preamble discussion only covers electronic versus paper, and commercial versus individual control. The FTC acknowledges that paper records can also be breached but does not feel that this product was intended to be covered by the statute.
- (e) ***PHR-identifiable health information*** means "individually identifiable health information," a definition taken from the Social Security Act which defines the term as "information that:
    - (1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse;
    - (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual."
- And, with respect to the individual:
    - (1) That is provided by or on behalf of the individual; and
    - (2) 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.
- (f) ***PHR-related entity*** means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that:
    - (1) Offers products or services through the Web site of a vendor of PHRs;
    - (2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals PHRs; or
    - (3) Accesses information in a PHR or sends information to a PHR.

- (g) ***State*** means any of the several states, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.
- (h) ***Third-party service provider means*** an entity that:
    - (1) Provides services to a vendor of PHRs in connection with the offering or maintenance of a PHR or to a PHR-related entity in connection with a product or service offered by that entity, and
    - (2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR-identifiable health information as a result of such services.
- (i) ***Unsecured*** means PHR-identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under section 13402 (b) (2) of HITECH.
    - **Author's Note:** This reference guidance was updated by the Secretary of HHS in the HHS (IFR) for Breach Notification for Unsecured Protected Health Information, issued on August 24, 2009 (http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf). The Preamble of this IFR (74FR42741-43) "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" includes not only an updated guidance from that issued in April 2009, but also a discussion on the guidance itself. HHS also indicates that future guidance will be issued via its Office of Civil Rights Privacy Web page at www.hhs.gov/ocr/privacy/. This Web page allows sign-up for notices when changes have been made. The HHS Preamble also provides examples on the use of encryption.
- (j) ***Vendor of personal health records*** means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity that offers or maintains a PHR.

Breach notification requirement—Section 318.3

This section addresses the general requirements of the Rule and how they relate to the following sections on timeliness, methods, and content.

- (a) ***In general*** each PHR vendor following the discovery of a breach of unsecured PHR-identifiable health information that is contained in an electronic PHR maintained or offered by the vendor, and each PHR-related entity following the discovery of a breach of security of such information that is obtained through a product or service provided by such an entity, shall:
    - Notify each individual who is a resident of the US and whose unsecured PHR-identifiable health information was acquired by an unauthorized person as a result of such breach of security; and
    - Notify the FTC.
        - **Author's Note**: subsection C (below) discusses breaches treated as discovered.
- **(b)** ***Third-party service providers,*** following the discovery of a breach of security, shall:
    - Provide notice of the breach to an official designated in a written contract by the vendor of PHR or the PHR-related entity, to receive such notices, or if such a

designation is not made to a senior official at the vendor of PHRs or PHR-related entity to which it provides services;
    - Obtain acknowledgement from the official that such a notice was received; and
    - In the notice, include the identification of each customer of the vendor of PHRs or PHR-related entity whose unsecured PHR-identifiable health information has been, or is reasonably believed to have been, acquired during such breach.
    - Vendors of PHRs and PHR-related entities shall notify third-party service providers of their status as vendors of PHRs or PHR-related entities subject to this Part.
        - Author's Note: The written contract here serves the same purpose as a business associate agreement under HIPAA. In the Preamble, the FTC notes its concern about such agreements and the need to identify individuals within the contract. PHR entities may want to include more than one identity to ensure the notice can be delivered in all situations. Note, that there is also a receipt process needed for the third-party service providers. More information on this is included in the Preamble (74FR42970-71).
- (c) ***Breaches treated as discovered***.
    - A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known by any of the three entities identified in this Rule.
    - Any of the three entities shall be deemed to have knowledge of a breach if such breach is known, or reasonably should have been known to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of PHRs, PHR-related entity, or third-party service provider.
        - **Author's Note**: A footnote (74FR42971) in the Rule's Preamble indicates that the FTC "expects entities that collect and store unsecured PHR-identifiable health information to maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner. If an entity fails to maintain such measures, and thus fails to discover a breach, the resulting failure to provide the appropriate breach notification could constitute a violation of the…rule because the entity 'reasonably' should have known about the breach. The Commission recognizes, however, that certain breaches may be very difficult to detect, and that an entity with strong breach detection measures may nevertheless fail to discover a breach. In such circumstances, the failure to discover the breach would not constitute a violation of the…rule."
        - **Author's Note**: The FTC does not address training where HHS does. While not specified, it should be assumed that the FTC would consider employee or agent training as an issue should a breach be uncovered but not identified by the covered entity.

Timeliness of Notification—Section 318.4

Following the requirements for determining a breach and the requirements for the affected entities the FTC addresses timeliness.

- (a) ***In general***, with the exception for law enforcement investigation, the notifications under Section 318.3 must be sent to the affected individual(s) without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.
- (b) ***Burden of proof.*** The vendor of PHRs, PHR-related entity, and third-party service provider involved in the breach will have the "burden of demonstrating that all notifications were made as required under this Part, including evidence demonstrating the necessity of any delay."
- (c) ***Law enforcement exception***. If a law enforcement official determines that a notification, notice, or posting, as required in this Rule, would impede a criminal investigation or cause damage to national security, then the notification, notice, or posting can be delayed. The FTC then requires the entity to follow HIPAA Privacy Rule Section 164.528 (a) (2), which essentially duplicates the requirements under the HHS version such that:
    - The exception in place for the time specified by an official if the official provides the covered entity with a written statement that such an accounting [notice] to the individual would reasonably impede the agency's activities and specifying the time for which such a suspension is required. The HIPAA requirement goes on to require that when the statement is oral the organization must:
        - Document the statement including the identity of the official making the statement;
        - Temporarily suspend the right to an accounting [notice] subject to the statement; and
        - Limit the temporary suspension to no longer than 30 days unless a written statement is submitted as required above.
        - Author's Note: The FTC approach is different than HHS's which spells out the obligation anew in the August 24 IFR requirements. In citing HIPAA, the FTC ignores the fact that Section 164.528 relates to the accounting of disclosures of PHI and not a notice or notification that is somewhat different than an accounting. Essentially, the requirements for all are the same relating to oral versus written statements and the time periods associated with each.

Methods of notice—Section 318.5

The FTC acknowledges that under its definition PHRs are electronic and with that given, it would make sense that the consumer—the individual who is the subject of the PHR—has the ability or desire to be contacted electronically, making the methods of notice here different than those required of HIPAA-related entities.

- (a) ***Individual notice***. A vendor of PHRs or a PHR-related entity that discovers a breach of security, as previously discussed, must provide a notice of such a breach to an individual promptly. The notice must follow the requirements in Section 318.3 and be in the following form.
    - (1) **Written notice, by first-class mail** to the individual at the individual's last known address, or **by e-mail** "if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice."

- If the individual is **deceased**, a notice must be provided to the individual's next-of-kin "if the individual had provided contact information for the next of kin, along with authorization to contact them."
- In any case, the notice may be provided in one or more mailings as information is available.
- **Author's Note:** As indicated, the FTC approach to notification is a departure from that of HHS. More detail on how this option is to be administered, including issues of spam security, can be found in the Preamble (74FR42972-73).
- (2) If "after making reasonable efforts to contact all individual to whom notice is required," the entity finds that contact information for 10 or more individuals is insufficient or out-of date, it shall provide substitute notice to "reach the individuals affected by the breach" in the following form:
  - (i) Through a conspicuous posting for a period of 90 days on the home page of its Web site; or
  - (ii) In major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside.
    - **Author's Note:** *Media* is defined as broadcast or print media, while use of Internet media is discouraged; the FTC believes the HITECH legislation only recognized print or broadcast media. The Preamble also raises the issue of identifying geographic media, but does not provide a conclusive answer to this issue.
  - The notice sent to the media or posted on the Web must include a toll-free phone number that must remain active for at least 90 days. Information on the toll-free number must allow an individual to learn whether or not the individual's unsecured PHR-identifiable health information may be included in the breach.
- (3) In any case where there is an "urgent" need to contact the individual because of "possible imminent misuse of unsecured PHR-identifiable health information," the entity may provide information to the individual by telephone or other appropriate means, in addition to the notice required in this section.

- (b) ***Notice to the media***. When there is a known breach of security or a reasonably believed breach has occurred which involves the unsecured PHR-identifiable health information of 500 or more residents of a state or jurisdiction, the vendor of the PHRs or PHR-related entity must provide a notice to prominent media outlets serving the state or jurisdiction.
  - **Author's note**: The notice to the media in this case is not the same as the notice for situations above where the media notice was an alternative notification. Here the requirement occurs as well as the individual notice requirement.
  - **Author's note**: In the Preamble (as with the HHS requirements) "jurisdiction" is a geographic area smaller than a state. Also, the 500 or greater number applies to a single state, so if the 500 or greater number cover more than one state, but no state has 500 or more, then no media notice may be required. See the Preamble (74FR 42974) for further discussion.
- (c) ***Notice to the FTC***. Vendors of PHRs, and PHR-related entities must provide notice to the FTC following the discovery of a breach of security of PHR-identifiable health information.

- If the breach involves **500 or more individuals**, then the notice must be provided as soon as possible and in no case later than 10 (ten) business days following the date of discovery.
- If the breach involved **less than 500 individuals**, the vendor of PHRs or a PHR-related entity may maintain a log of any such breach and submit such a log annually to the FTC no later than 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year.
- **Instructions** for these notifications will be provided at the FTC Web site.
  - **Author's note**: The FTC actually included the notification form for either the 10-day or log notification with its Final Rule. This can be found at 74FR429.83-85, please read these instructions closely as there may be a need for more than one submission. The form also provides contact information for questions related to the report in the form of a phone number (202) 326-2252 or an e-mail hbn@ftc.gov.

Content of notice—Section 318.6

The FTC Rule has a short set of requirements for the content of a notice of breach no matter which method is used. The notice for a breach of security must be in plain language and include, to the extent possible:

- "(a) A brief description of **what happened**, including the date of the breach, and the date of the discovery of the breach, if known;
- (b) A description of the **types of** unsecured PHR-identifiable health **information** that were involved **in the breach** (such as full name, Social Security number, date of birth, home address, account number, or disability code);
- (c) **Steps individuals should take** to protect themselves from potential harm resulting from the breach;
- (d) A brief description of **what the entity** that suffered the breach **is doing** to investigate the breach, to mitigate harm, and to protect against any further breaches; and
- (e) **Contact procedures** for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address."
- **Author's Note**: In citing the content, the FTC in the Preamble also notes that the actual information should not be repeated in the notice. The Commission also notes that entities should use clear language and syntax in their notice and not include any extraneous material that might diminish the message they are trying to convey.

Enforcement—Section 318.7

This short section notes that "a violation of this Part shall be treated as an unfair or deceptive act or practice in violation of a regulation under Section 18 (a) (1) (B) of the Federal Trade Commission Act (15 USC 57 (a) (1) (B) regarding unfair or deceptive acts or practices." Nowhere does the Commission get specific in the penalties that could be forthcoming for a violation. The FTC's enforcement work is done through administrative proceedings and in federal court actions.

Effective date—Section 318.8

As noted above the **effective date** for this Part is **September 24, 2009**. The FTC has noted, however, that it "will use its enforcement discretion to refrain from bringing an enforcement action for failure to provide the required notifications for breach that are discovered before February 22, 2010. During this initial time period—after this rule has taken effect but before an entity is subject to an enforcement action—the Commission expects regulated entities to come into full compliance with the final rule."

Sunset—Section 318.9

This section reflects Congress' statute language that signifies these regulations are "temporary" pending legislation that may come forward that would affect the three entities covered by this Part. Although not stated in this Rule, there has been discussion (but no legislation) in Congress to bring all healthcare-related privacy requirements, including breach notification under HIPAA.

Preamble to the Breach Notification

Preambles are written for most final rules to provide the background for the rule as it is presented. The FTC's preamble to this rule is relatively short and relies on knowledge of the NPRM from April of 2009.

I. Background (74FR42962)

This background section essentially notes the legislative history for HITECH and the fact that this legislation calls for "temporary requirements" to be enforced by the FTC for the non-HIPAA related entities named in the legislation.

II. Overview of the Recovery Act, Proposed Rule, and Comments Received (74FR42962-63)

The FTC notes which entities are the subjects for the Commission's rule making—namely PHR vendors, PHR-related entities, and third-party service providers of the former two. The FTC also notes that HHS is required to provide a similar set of recommendations for HIPAA-related entities and both agencies are required to report back to Congress on issues surrounding the privacy and security of health records.

Responding to comments on its NPRM, the FTC essentially makes five comments.

- The FTC and HHS recognized that there would be overlap between their rules and, therefore, it was prudent to work together;
- There would be situations where, due to overlap between the FTC and HHS, a consumer might receive more than one notice—suggesting that steps should be set up to ensure that in the case of an overlap the consumer would not receive multiple notices for the same event;
- That it (the FTC) will not be undertaking privacy and security rulemaking for PHRs as this was not the intention of Congress;
- That it will not address concerns regarding electronic records in general; and

- That it cannot change the statutory language, however, it will take comments into "account" when providing input into the joint report with HHS.

III. Description of Interim Final Rule (74FR42743)

As noted, the FTC's overview is relatively simple. It 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.

Purpose and Scope (Section 318.1)

This section identifies the statutory authority and the FTC responds to several comments:

- The final Rule has been clarified to note that it applies to vendors of PHRs and PHR-related entities, "irrespective of any jurisdictional tests in the Federal Trade Commission Act."
- The final Rule does not apply to HIPAA-covered entities (including the Federal government) and this section provides some discussion on the issue of overlap between the FTC and HHS rules especially as they relate to business associates and how notices might be sent in different situations.
- Foreign entities with US customers must provide breach notification under US laws.
- Under Section 13421 of HITECH there is preemption as applies to HIPAA for contrary situations.

Definitions (Section 318.2)

The section on Definitions includes:

- **Breach of security**—FTC uses the definition provided in the NPRM, and decided to adopt a "rebuttable presumption" as part of the definition. However, the FTC also notes "because health information is so sensitive, the Commission believes the standard to notification must give companies the appropriate incentive to implement policies to safeguard such highly sensitive information." The FTC also warns vendors of circumventing the intent of the legislation through authorizations buried in consent or disclosure documents noting that it "expects that vendors of personal health records and PHR-related entities would limit the sharing of consumers' information, unless the consumers exercise meaningful choice in consenting to such sharing."
    - **Author's Note**: The concept of "rebuttable presumption" is discussed at length in the Rule's Preamble, for those not familiar with this approach.
- **Business associates and HIPAA-covered entities**—Are defined under HIPAA.
- **Personal health record**—In this Rule the definition applies only to *electronic* PHRs.
- **PHR-identifiable health information**—adopts the "identifiable health information" definition that is in HIPAA. There is considerable discussion (74FR42968-69) under this title in the Preamble giving the Commission's reflection on just what, potentially, is identifiable health information in the context of PHR products including "de-identified" data.
- **PHR-related entity**—in addition to adopting the proposed definition that a "PHR-related entity: "(1) offers products or services through the Web site of a vendor of personal health records; (2) offers products or services through the Web sites of HIPAA-covered entities that offer individuals PHRs; or (3) accesses information in a personal health record or sends

information to a personal health record; the FTC also notes that search engines are PHR-related entities if they appear on PHR Web sites. In this case they are subject to the Rule if they collect unsecured PHR-identifiable information at those Web sites. In a footnote the FTC goes on to say that a consumer authorized family member who accesses information in a consumer's PHR is not considered a PHR-related entity.

- **State—**takes on the usual definition of the 50 states, plus the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.
- **Third-party service provider—**the discussion covers what services are considered applicable to qualify as a third-party service provider (74FR42969).
- **Unsecured**—this term applies to guidance provided by the Secretary of HHS. As noted above, this guidance was renewed in the August 24 IFR provided by HHS (74FR42741-43) and will be updated at the HHS Web site www.hhs.gov/ocr/privacy.
- **Vendor of personal health records**—the FTC retains its proposed definition (above) and received limited comment.

Breach notification requirement (Section 318.3)

This section (74FR42970-71) highlights some of the comments and resolutions associated with the original NPRM for the Rule:

- The FTC notes that it has added the requirement that vendors of PHRs and PHR-related vendors must notify third-party service providers of their status as vendors of PHRs or PHR-related entities.
- The third-party service provider is required to identify each "customer of the vendor of personal health records or PHR-related entity" whose information was breached. In stating this, the FTC is requiring such entities to be able to identify the individual as well as their respective vendor or PHR-related entity.
- A specific individual must be identified to receive a report of a breach from a third-party service provider.
- A third-party service provider must receive a receipt from the vendor or PHR-related entity.
- The FTC provides some examples of when a breach should be treated as discovered.

Timeliness of Notification (Section 318.4)

Most of the discussion in this section (74FR42971) deals with timeliness and reasonableness. First the Commission notes "an entity need not establish all the prerequisites for triggering a breach notification before the 60 day time period starts;" meaning that the time begins at discovery and not at the completion of an investigation. Secondly, the breach is considered "discovered" at the point when an entity reasonably should have know about it. Several examples accompany this discussion.

Methods of Notice (Section 318.5)

- ***Notice to the Individual***—The Preamble provides a lengthy discussion (74FR42971-74) as to the FTC's rationale for the specific requirements in the Final Rule. The length of this discussion, in part, has to do with this being the breach related to an electronic product, and where it is assumed the customer may desire electronic communication (notice) rather than

by surface mail. In addition, there is a conversation concerning the amount of information actually collected from an electronic PHR customer such as addresses, other contact information, or next-of-kin information. Accordingly, this section of the FTC rule is significantly different than that in the HHS rule, although there is nothing prohibiting the requirements in the HHS rule from meeting the requirements of the FTC rule.

- ***Notice to the Media if the Breach Affects 500 or More Individuals*—**Most of the discussion in this section (74FR42974) deals with the definition of "State or jurisdiction" and the idea of using Internet media. In the former discussion, the FTC provides the previous definition of a state and then qualifies the requirement based on the number of individuals residing in a state such that even though an entity might have a breach of greater than 500, if no one state has 500 or more there may not be a requirement to provide notice to the media.

The latter discussion deals with whether Internet media can be used in lieu of print or broadcast media. The Commission says that it cannot.

- ***Notice to the Commission***—This section (74FR42974-75) is rather straightforward. The Commission extended the timeline for reporting breaches of 500 or more from 5 days to 10. The commission also clarifies its reporting period and deadline for the logs that must be submitted, and highlights its reporting form, which was attached to the Final Rule.

Content of Notices (Section 318.6)

This is a rather straight-forward section (74Fr42975-76) laying out the final requirements for the notice content including the need for the notice to be written in plain language.

Enforcement, Effective Date, and Sunset (Sections 318.7, 318.8, and 318.9)

The Preamble merges these three sections into a very brief discussion (74FR42976), which for the most part echoes the description above in the Rule itself.

IV. Paperwork Reduction Act (74FR42976)

This is a required discussion for all final rules. In it the Commission describes how it must go about seeking the approval from the Office of Management and Budget (OMB) as well as the practical utility of the Rule and an explanation of the burden estimated under the Final Rule. This is a very limited discussion that includes staff estimates for cumulative breaches in a year's time—11—and what cost estimates were arrived at on this basis.

V. Need for and Objectives of the Rule (74FR42978)

Again, this is a required discussion which the FTC addresses in quick fashion essentially with the same discussions as in prior sections. The Commission notes that the objective for the Rule was raised in the HITECH legislation and that it received no substantive comments on the Rule or its analysis.

The FTC goes on to point out who will be covered by the Rule and its requirements, as well as what steps the Commission has taken to minimize any significant economic impact on small entities.

MORE TO COME

This is a not only a new Rule, it is a new agency overseeing a fairly new product with a parallel environment in the form of similar Rules within the healthcare (HIPAA) structure. Watch *AHIMA's e-Alert* and ARRA Web site for further information.