

Expansive New HHS And FTC Regulations Require Entities To Provide Notice Of Data Breaches Involving Health Information

Jo-Ellyn Sakowitz Klein

AKIN GUMP STRAUSS HAUER &
FELD LLP

The Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) recently issued significant regulations implementing provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA). HHS published its much-anticipated breach notification rule on August 24, 2009. These new regulations, to be codified at 45 C.F.R. Part 164, Subpart D, apply to hospitals, health plans, health care clearinghouses and other covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as to their business associates. Stakeholders are invited to comment on the HHS rule, which was issued as an interim final regulation, and comments are due on or before October 23, 2009. The FTC published a separate health breach notification final rule governing vendors of personal health records (PHRs) and certain PHR related entities on August 25, 2009, to be codified at 16 C.F.R. Part 318, which followed a proposed rule that was published on April 20, 2009.

The HHS rule becomes effective on September 23, 2009, and the FTC rule becomes effective September 24, 2009. Acknowledging that it will take time for entities to develop and implement the procedures needed to comply with these regulations, both agencies agreed to refrain from imposing sanctions for failure to provide required notifications for breaches discovered before February 22, 2010.

Notwithstanding this enforcement delay, affected entities should take prompt action to come into compliance. HHS clarified that entities are expected to be in compliance beginning on September 23, 2009, and noted that the agency would work with entities, through technical assistance and voluntary corrective action, to achieve compliance. Notably, covered entities are required to submit breach notification logs to HHS on an annual basis, and these logs must contain information on breaches occurring on or after September 23, 2009. The FTC similarly noted that regulated entities are expected to come into full compliance during the enforcement hiatus and that annual logs due to the FTC must include information for breaches occurring after the effective date of the regulation.

This article provides an overview of the relevant statutory requirements, highlights key provisions of the HHS and FTC breach notification regulations and presents some ideas for steps affected entities may want to take as they move

Jo-Ellyn Sakowitz Klein is Counsel in the Washington, DC office of Akin Gump Strauss Hauer & Feld LLP. Her practice is devoted to regulatory, transactional and legislative matters affecting the health industry.

forward with their compliance efforts.

HHS Rule: Breach Notification For Unsecured Protected Health Information

Overview of the Statutory Requirements

ARRA establishes an expansive protocol for providing notice in the event that an individual's unsecured protected health information (PHI) has been (or is reasonably believed to have been) accessed, acquired or disclosed as a result of a breach. The statutory regime is more prescriptive and onerous than data breach notification laws presently in place in many states. Depending on the circumstances, breach notification must be provided to individuals, HHS and/or the media.

For the purposes of the statute, a breach is defined as the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information, subject to three rather narrow exceptions: (1) unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a covered entity or business associate, provided that the acquisition, access or use was made in good faith, within the course and scope of employment (or other professional relationship), and does not result in further use or disclosure; (2) inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility to another similarly situated individual at the same facility, provided that the information is not further used or disclosed; and (3) situations where the recipient of the information would not reasonably be able to retain the information. The statute also creates a safe harbor for breaches involving PHI that has been secured through the use of certain technologies and methodologies HHS has identified as rendering PHI unusable, unreadable or indecipherable to unauthorized individuals.

The statute prescribes the timing, manner and content for the required notices in remarkable detail. For example, notice must be sent to individuals – without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, via first-class mail (or, if specified as a preference by the individual, by e-mail) – and must contain, to the extent possible: (1) a brief description of what happened, including when the breach happened and when it was discovered; (2) a description of the types of PHI that were compromised (e.g., full name, Social Security number, date of birth, home address, account number or disability code); (3) the steps individuals should take to protect themselves from potential harm relating to the breach; (4) a brief description of what the covered entity is doing to investigate the breach, mitigate the harm and prevent future breaches; and (5) a toll-free number, e-mail address, Web site or postal address individuals can use to obtain additional information. The statute continues to describe rather elaborate substitute notice procedures that must be followed where the required notice cannot be furnished because contact information

available for the affected individual is insufficient or out-of-date. The statute further specifies that in any case deemed by the covered entity to require urgency (e.g., due to imminent misuse of the PHI involved), the covered entity may contact the affected individuals by telephone or other means, as appropriate, but must still provide the required written notice.

Moreover, the statute dictates that for breaches involving 500 or more individuals, the covered entity must notify HHS immediately. And, where the breach involves more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets serving the state or jurisdiction, within the same timeframe that it notifies individuals. For breaches involving fewer than 500 individuals, covered entities must maintain a log of such breaches and submit this log to HHS annually.

The statute contains mandates for business associates (such as billing services or third party administrators) as well as for covered entities. Business associates that discover breaches must notify the covered entity of the situation. These notices must identify each individual whose unsecured PHI has been (or is reasonably believed by the business associate to have been) accessed, acquired or disclosed during the breach. Notably, the statute applies the same 60-day standard to business associates as it applies to covered entities.

Highlights of the HHS Breach Notification Rule

Through its rulemaking, HHS made several important clarifications to the statutory breach notification requirements, and also updated its guidance published on April 27, 2009, specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. Highlights include

- **Harm threshold and risk assessment.** HHS established a harm threshold, which allows covered entities and business associates to forego notification if they determine an incident poses little or no risk of harm to the individual whose PHI was involved (i.e., in terms of the definition of breach, the incident did not compromise the security or privacy of the information). Under this standard, a covered entity or business associate would need to perform a risk assessment to determine whether an unauthorized acquisition, access, use or disclosure poses a significant risk of financial, reputational or other harm to the individual. HHS described several factors that covered entities and business associates should consider in their risk assessments, including considering who received the PHI (e.g., a hacker versus another covered entity); any mitigation efforts that may reduce the likelihood of harm; whether the PHI (or media storing the PHI) was returned prior to access or use; and the nature of the PHI disclosed. HHS emphasized that risk assessments should be fact-specific and must be documented.

- **Updates to guidance specifying how to render PHI secure.** Under ARRA, breach notification is only

required in situations where the PHI subject to the breach is "unsecured." In this rule, HHS updated its April 27, 2009, guidance addressing the technologies and methodologies that render PHI secure. Although HHS considered suggestions as to alternate technologies that would render PHI secure, the agency decided that encryption and destruction remain the only two technologies or methodologies that it will recognize as valid ways of removing records from the realm of "unsecured" PHI. HHS explicitly rejected redaction as an acceptable alternative to secure paper-based PHI. Under ARRA, HHS must update this guidance annually, and the first annual update will be issued in April 2010.

- **Refinements to exceptions.** HHS made important modifications to the rather narrowly worded statutory exceptions to what types of uses and disclosures constitute a breach. The exceptions now arguably encompass more situations where a use or disclosure was truly accidental, occurred internally or presents relatively little risk of harm. The exception for unintentional access by an employee of a covered entity or business associate has been expanded to include all workforce members, not just employees. The exception for inadvertent disclosures among similarly situated employees has been construed to cover inadvertent disclosures made by an authorized person within a covered entity or business associate to another similarly authorized person within the same covered entity, business associate or organized health care arrangement (OHCA) – even where the disclosure crosses state lines because the entity has multiple locations across the country. Finally, HHS clarified that breach notification is not required where the covered entity or business associate believes in good faith that the unauthorized recipient of the PHI would not reasonably have been able to retain the information. Covered entities and business associates seeking to take advantage of these exceptions must document their analyses.

- **Breaches involving limited data sets.** HHS declined to treat limited data sets (as defined in the relevant regulations) as secured for purposes of the safe harbor, but provided a narrow exception for unauthorized uses or disclosures involving limited data sets from which certain additional data elements have been excluded. If the information used or disclosed without authorization constitutes a limited data set, and the information also does not include the individual's date of birth or zip code, then the PHI is not considered compromised for breach notification purposes. By contrast, if the date of birth and zip code identifiers are included in the limited data set, the covered entity or business associate would still have to undertake a risk assessment that would include an analysis of whether the data set could be used to identify the individual.

- **When breaches are treated as discovered.** Affected entities will need to act promptly when faced with a breach, as notices to individuals must be pro-

Please email the author at jsklein@akingump.com with questions about this article.

vided without unreasonable delay and in no case later than 60 calendar days following discovery of the breach. HHS specified that breaches will be treated as discovered on the first day the breach is known to the covered entity or business associate or, by exercising reasonable diligence, would have been known to the covered entity or business associate. Significantly, under the rule, an entity is deemed to have discovered the breach when any member of its workforce or an agent (other than the person committing the breach) first learns of the breach or, by exercising reasonable diligence, would have known of the breach. Accordingly, it will be vital for institutions to have appropriate internal reporting systems in place, as well as clear lines of communication established with any outside agents. The rule also clarifies that the 60-day period begins when the incident is first known, not when the investigation of an incident is complete – thus, the 60-day period begins to run even if it is initially unclear whether the incident constitutes a breach as defined by the rule.

• **Requirements for business associates.** Following discovery of a breach, a business associate is required to notify the covered entity of the breach so that the covered entity can provide required notices. The rule clarifies that, for business associates that maintain PHI on behalf of more than one covered entity, it is only necessary to notify the covered entity to which the PHI relates. The rule also builds upon the statutory requirements to require that business associates, in addition to identifying the individuals whose PHI was involved in the breach, also provide a covered entity with any other available information that the covered entity is required to include in its notification.

Rule: Health Breach Notification For PHR Vendors and PHR-Related Entities

Overview of the Statutory Requirements

ARRA requires vendors of PHRs and certain PHR related entities to notify their customers following discovery of a breach of security of unsecured PHR identifiable health information that is in a PHR. ARRA specifies that failure by these entities to provide required notices will be treated as an unfair and deceptive act or practice in violation of the Federal Trade Commission Act.

ARRA elaborates on the meaning of a breach of security, specifying that the breach notification requirements will be triggered by the unauthorized acquisition of unsecured PHR identifiable health information of an individual in a PHR. The statute further provides that PHR identifiable health information is defined as individually identifiable health information (as defined by relevant regulations) that is provided by or on behalf of the individual and that identifies the individual (or can be used to identify the individual). A PHR – unlike an electronic health record (EHR), which is generally created and used by health care providers – is an electronic health record that can be drawn from multiple sources and is managed, shared and controlled by or primarily for the individual.

The ARRA provisions concerning breaches involving PHRs generally mirror those prescribed for PHI, in terms of the timeliness, methods and content of the notification. For instance, upon dis-

covery of a breach, a PHR vendor or PHR related entity is required to notify each individual whose unsecured PHR identifiable health information was subject to the breach, and must maintain a log of all such breaches for annual submission to the FTC. Also, like the provisions concerning PHI, for breaches involving 500 or more individuals, PHR vendors and PHR related entities must provide notice to prominent media outlets and to the FTC. The FTC, in turn, is required to alert the Secretary of HHS. Third party service providers have responsibilities similar to those assigned to HIPAA business associates and are required to notify the PHR vendor or PHR related entity of the breach. And, as with breaches involving PHI, notices are generally required to be furnished without unreasonable delay and in no case later than 60 days following discovery of the breach.

The breach notification provisions covering PHRs were intended to serve as a temporary fix to address a gap existing because PHR vendors and PHR related entities are generally not subject to HIPAA. ARRA directs the FTC to work with HHS to report to Congress by February 17, 2010, on potential privacy, security and data breach notification requirements for entities not currently subject to HIPAA. ARRA also provides that the breach notification requirements applicable in the PHR realm will sunset if Congress enacts new legislation establishing notice requirements that would apply to PHR vendors and related entities sustaining a breach of security.

Highlights of the FTC Breach Notification Rule

The FTC's final health breach notification rule expands on the statutory requirements and responds to comments received on the proposed rule. The FTC follows the HHS guidance on when data is considered secured, so that issue is not addressed in a material fashion in the FTC rule. Highlights of the FTC breach notification rule include –

• **Clarification of the types of entities to which the FTC rule applies.** The FTC rule clarifies that it primarily applies to two categories of entities: PHR vendors and PHR related entities. PHR vendors offer or maintain PHRs. PHR related entities offer products or services through the Web site of a PHR vendor, offer products or services through the Web sites of HIPAA-covered entities that offer individual PHRs, or access information in, or send information to, a PHR. Notably, an entity that advertises on a PHR vendor Web site may be subject to the FTC rule if it collects information through the Web site, for example if it offers a search engine that tracks customers' IP addresses or previous searches.

• **Obligations of third party service providers.** Third party service providers – the FTC analog to business associates – are individuals or entities that furnish services either to PHR vendors in connection with the offering or maintenance of PHRs, or to PHR related entities in connection with a product or service offered by that entity, and that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHR identifiable information as a result of such services. The FTC builds on the statute to specify that these entities must provide breach notifications to an official designated – in a written contract by the

PHR vendor or PHR related entity – to receive such notices. If no official is so designated, notice must be furnished to a senior official of the entity, and receipt of the notice must be acknowledged.

• **Rebuttable presumption.** One key distinction between the FTC and HHS rules is that the FTC rejected HHS' harm threshold for determining whether privacy or security has been compromised as a result of a breach. The FTC does afford regulated entities a degree of flexibility by building a rebuttable presumption into the definition of what constitutes a breach. The FTC rule provides that 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 where there is unauthorized access to unsecured PHR identifiable information, unless the PHR vendor, PHR related entity or third party service provider that experienced the breach has reliable evidence demonstrating that there has not been (or could not reasonably have been) unauthorized acquisition of the information.

• **Exception for inadvertent access by employees.** The FTC noted that in cases of inadvertent access by an employee, breach notification is not required if the employee follows company policies by reporting such access to his or her supervisor and affirming that he or she did not read or share the data. The company must also conduct a reasonable investigation to corroborate the employee's version of events.

• **No reasonable basis to identify individuals.** The FTC declined to treat limited data sets as having been removed from the realm of PHR identifiable information, but instead noted that breach notification may not be required where an entity can demonstrate that there is no reasonable basis to identify individuals whose data has been breached.

• **When breaches are treated as discovered.** The FTC shared HHS' approach to when breaches should be treated as discovered. Breaches will be treated as discovered on the first day on which the breach is known (or reasonably should have been known) to the PHR vendor, PHR related entity or third party service provider, and an entity will be deemed to have knowledge of a breach if the 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 the entity.

• **Guiding principles.** The FTC expressed several themes in the preamble to the final rule, including that consumers should generally receive a single breach notice for a single incident, and that notice should come from the entity with which the consumer has a direct relationship (rather than from an entity that has been invisible to the consumer). The FTC also provided some insights as to when a use or disclosure of information contained in a PHR would be considered unauthorized, which is somewhat more complicated in the PHR context than in the PHI context, because no regulations exist dictating when authorization for use or disclosure of PHR identifiable health information is required.

• **Scope of the FTC's authority and jurisdiction.** The FTC explained that its enforcement power relating to the data

breach notification rule extends to non-profit entities, as well as to foreign entities that maintain information on U.S. citizens or residents.

Coming Into Compliance

The fact that neither HHS nor FTC plans to impose sanctions with respect to breaches discovered before February 22, 2010, should not deter affected entities from taking prompt action to address these new federal regulatory requirements. HHS and FTC both seem increasingly committed to enforcing privacy and security regulations in the health care context. Since the change in administration, we have seen the FTC settle charges against retail pharmacy chain CVS Caremark for failing to secure sensitive customer medical information appropriately, and announce its intent to enforce its anti-identity theft rule – the Red Flags Rule – in the health sector. Similarly, in recent months, HHS has consolidated authority for enforcing security as well as privacy regulations within its Office for Civil Rights (OCR) and solicited applications for several newly created OCR enforcement positions.

As a first step, entities should evaluate whether they are subject to the HHS rule, the FTC rule or, perhaps, to both rules. It is quite clear that the HHS rule applies only to HIPAA-covered entities and business associates. Less clear, however, is when the FTC rule will come into play. The FTC rule provides that it will not apply to "HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity" (emphasis added). Indeed, the regulators recognized that some entities may be subject to both rules, as when, for example, a business associate of a HIPAA-covered entity also offers PHRs directly to the public.

Next steps for affected entities could include updating policies and procedures to incorporate the breach notification responsibilities, and training all workforce members accordingly. Affected entities should also develop and disseminate internal policies designed to encourage workforce members to report suspected breaches immediately through established internal channels, so the entity can make a prompt decision about how to respond. Affected entities may also find it helpful to prepare a notification template to use in the event of a breach, which should take both federal and state breach notification laws into account. Affected entities should also review their business associate and service provider agreements to evaluate the extent to which amendments are needed in light of the new notification obligations.

In addition, affected entities should consider commenting on the HHS breach notification rule. While the regulations seem rather exhaustive, there are some areas where additional agency input may be needed. For example, while HHS clarified that a HIPAA privacy violation is necessary, but not sufficient, to trigger the breach notification requirements, agency guidance may be helpful concerning whether entities reporting breaches to HHS as required by law will have to bear the full brunt of penalties for underlying HIPAA violations revealed, among other issues. As noted above, the comment period remains open until October 23, 2009.