

HHS, FTC ISSUE BREACH NOTIFICATION RULES FOR ELECTRONIC HEALTH INFORMATION

On August 19, 2009, the U.S. Department of Health and Human Services ("HHS") issued an interim final rule with a request for comments ("HHS Rule") requiring covered entities under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and their business associates to notify individuals of breaches of unsecured protected health information ("PHI").¹ The Federal Trade Commission ("FTC") issued a similar final rule ("FTC Rule") applicable to vendors of personal health records ("PHR"), PHR related entities, and third party services providers on August 17, 2009.² These regulations implement provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act" or "Act"), passed as part of the American Recovery and Reinvestment Act of 2009.³

The HHS Rule will take effect on September 23, 2009, and the FTC Rule will take effect on September 24, 2009. However, HHS and the FTC will use their enforcement discretion to refrain from imposing sanctions for failure to provide the required notification for breaches that are discovered before February 22, 2010. The FTC and HHS expect regulated entities to use this time to come into full compliance with the applicable rules.

I. SCOPE OF THE BREACH NOTIFICATION RULES

The HHS Rule applies to HIPAA-covered entities and their business associates that access, maintain, retain, record, store, describe, destroy, or otherwise hold, use, or disclose unsecured PHI.⁴ Under HIPAA and the privacy rule implemented thereunder (the "HIPAA Privacy Rule"), an entity is a "covered entity" if it is a health plan, a health care provider that engages electronically in transactions that have been standardized under HIPAA, or a health care clearinghouse.⁵ A "business associate" is an entity that performs, on behalf of a covered entity, functions involving the use or disclosure of PHI.⁶

The FTC Rule applies to foreign and domestic vendors of PHR,⁷ PHR related entities,⁸ and third party service providers⁹ that maintain information of U.S.

¹ Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160 & 164).

² Health Breach Notification Rule, 74 Fed. Reg. 42,962 (Aug. 25, 2009) (to be codified at 16 C.F.R. pt. 318).

³ Pub. L. 111-5.

⁴ 74 Fed. Reg. at 42,740. The HITECH Act incorporates the definitions of "covered entity," "business associate," and "protected health information" used in HIPAA.

⁵ 45 C.F.R. § 160.103.

⁶ *Id.*

⁷ A vendor of PHR is an entity that offers or maintains a PHR. A PHR, in turn, is an electronic record of 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. 74 Fed. Reg. at 42,980.

⁸ A PHR related entity is an entity that: (1) offers products or services through the website of a vendor of PHR; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHR; or (3) accesses information in a PHR or sends information to a PHR. *Id.*

citizens or residents. The rule applies to such entities without regard to whether they fall under the FTC's traditional jurisdiction under section 5 of the FTC Act.¹⁰

To address the limited cases where an entity is subject to both the HHS and FTC Rules (*e.g.*, an entity that provides PHRs to customers of a HIPAA-covered entity as a business associate, but also provides PHRs to the public as direct customers), the agencies worked together to harmonize the two rules, within the constraints of the statutory language.¹¹ Where a PHR vendor or PHR related entity (1) provides notice of a breach on behalf of a HIPAA-covered entity; (2) has dealt directly with these consumers in managing the PHR account; and (3) provides such notice at the same time as it provides an FTC-mandated notice to its direct customers, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be compliance with corresponding FTC Rule provisions.¹² The FTC Rule provides detailed guidance regarding situations of dual or overlapping coverage between the FTC and HHS Rules.

Notably, the breach notification requirements in the HHS and FTC Rules apply to only *unsecured* PHI or PHR identifiable health information,¹³ respectively. For purposes of both rules, "unsecured" means data that is not secured through use of a technology or methodology specified in HHS guidance.¹⁴ In guidance issued on April 17, 2009, HHS identified encryption and destruction as the only two methodologies currently available to render information unusable, unreadable, and undecipherable.¹⁵ Compliance with the guidance yields a significant benefit: if an entity secures data pursuant to the guidance and later discovers a breach, the entity would not be required by the HHS and FTC Rules to provide breach notification because the data falls outside the scope of the Rules.

II. HHS BREACH NOTIFICATION RULE AND UPDATED GUIDANCE

The HHS Rule closely tracks the breach notification requirements in the HITECH Act. The Act provides that, within 60 calendar days after the discovery of a breach of unsecured PHI, covered entities must notify any individual whose PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of the breach.¹⁶ Business associates must similarly notify covered entities following the discovery of a breach of unsecured PHI.¹⁷

⁹ A third party service provider is an entity that (1) provides services to a PHR vendor in connection with the offering or maintenance of a personal health record 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. *Id.*
¹⁰ *Id.*

¹¹ The FTC agreed with multiple commenters to its proposed rule, at 74 Fed. Reg. 17,914 (Apr. 20, 2009), who expressed that customers should receive a single breach notice for a single breach, and the breach notice should come from the entity with whom the consumer has a direct relationship.

¹² *Id.* at 42,964.

¹³ "PHR identifiable health information" is defined as "individually identifiable health information" under HIPAA, and, with respect to an individual, information that (1) is provided by or on behalf of the individual; and (2) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. *Id.* at 42,980.

¹⁴ *Id.* at 42,980, 42,768.

¹⁵ Guidance Specifying Technologies and Methodologies that Render Protected Health Information Unusable, etc., 74 Fed. Reg. 19,006 (Apr. 27, 2009). To access a previous Covington E-Alert about the HHS guidance, [click here](#).

¹⁶ HITECH Act, § 13402. Notification can be delayed if it would impede a criminal investigation or damage national security.

¹⁷ *Id.*

A. Unauthorized Acquisition of Data

For HHS-regulated entities, the HITECH Act defines a “breach” as the unauthorized acquisition, access,¹⁸ use, or disclosure of PHI which compromises the security or privacy of such information, subject to several exceptions. Under the HHS Rule, “unauthorized acquisition, access, use or disclosure of PHI” is defined as an impermissible use or disclosure under the HIPAA Privacy Rule.¹⁹ A violation of the HIPAA Security rule does not itself constitute a breach under the HHS Rule, but such a violation may lead to an impermissible use or disclosure under the HIPAA Privacy Rule and thus constitute a breach.

The HHS Rule excepts from the definition of “breach” the following three situations: (1) where PHI is unintentionally acquired, accessed, or used by a workforce member or person acting under the authority of an HHS-regulated entity, if such access is made in good faith and within the scope of authority, and does not result in further unauthorized use or disclosure -- *e.g.*, a billing employee receives and opens an e-mail containing PHI which a nurse mistakenly sent to him, alerts the nurse of the misdirected e-mail, and deletes it; (2) where a person who is authorized to access PHI at an HHS-regulated entity inadvertently discloses the PHI to another similarly situated individual at the same facility, but the disclosure does not result in further unauthorized use or disclosure -- *e.g.*, a physician who has authority to use or disclose PHI at a hospital by virtue of participating in an organized health care arrangement with the hospital inadvertently discloses PHI to a nurse who works at the hospital; and (3) where PHI is disclosed to an unauthorized person and the HHS-regulated entity has a good faith belief that the person would not reasonably have been able to retain the information -- *e.g.*, a covered entity sends explanations of benefits (“EOBs”) to the wrong individuals and the EOBs are returned by the post office, unopened, as undeliverable.²⁰

HHS agreed with commenters that the statutory language, “compromises the security or privacy of such information,” encompasses a harm threshold, and therefore clarified in the Rule that an impermissible use or disclosure constitutes a breach if it poses a significant risk of financial, reputational, or other harm to the individual.²¹ According to HHS, the inclusion of a harm threshold will lead to better consistency and alignment with state laws. Thus, to determine if an impermissible use or disclosure of PHI constitutes a breach, HHS-regulated entities will need to perform a risk assessment to ascertain whether there is a significant risk of harm to the individual.²²

In addition, the Rule provides a narrow exception to what compromises the security or privacy of PHI for a use or disclosure of PHI that excludes the 16 direct identifiers listed for limited data sets, as well as dates of birth and zip codes.²³ HHS has determined that PHI stripped of such identifiers poses a low level of risk of harm to the individual; therefore, notification in the event of a breach is unnecessary.

¹⁸ Neither the Act nor the HHS Rule defines the terms “acquisition” or “access.”

¹⁹ 74 Fed. Reg. at 42,767. The terms “use” and “disclosure” are defined broadly under the HIPAA Privacy Rule to include, for example, “examination” and “provision of access,” respectively. 45 C.F.R. § 160.103.

²⁰ 74 Fed. Reg. at 42,746-48, 42,767-68.

²¹ *Id.* at 42,767.

²² HHS also provides a three-part analysis for determining whether a breach has occurred: (1) Has there been an impermissible use or disclosure of PHI under the Privacy Rule?; (2) Does the impermissible use or disclosure compromise the security of the PHI (*i.e.*, is there a significant risk of financial, reputational, or other harm to the individual)?; and (3) Does the incident fall under one of the exceptions to the breach definition?

²³ *Id.*

B. Notification to Individuals

The HHS Rule provides that a breach is considered “discovered” for the purpose of the time period for notification as of the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known.²⁴ The Rule attributes knowledge of a breach by any workforce member²⁵ or other agent (as determined under the federal common law of agency), including certain business associates, to the covered entity itself. Thus, covered entities should implement reasonable systems for discovering breaches and train employees and agents to timely report privacy and security incidents.

Although HHS declined to impose a page limitation for the breach notice, the final rule requires the notice to be written in plain language.²⁶

C. Notification to Media

The HHS Rule requires a covered entity to notify prominent media outlets within 60 days of a breach involving 500 or more residents of a state or jurisdiction.²⁷ What constitutes a prominent media outlet will differ depending on the state or jurisdiction affected. The Rule includes clarification on how to address a breach involving residents in multiple states or jurisdictions. For example, if a breach involves the PHI of 600 Maryland residents and 600 District of Columbia residents, notification must be provided to prominent media outlets serving both Maryland and the District of Columbia. But if a breach involves the PHI of 200 Maryland residents, 200 Virginia residents, and 200 District of Columbia residents, notification to the media is not required; however, the entity still must notify individuals and HHS.

D. Notification to HHS

For breaches involving 500 or more individuals, the HITECH Act requires covered entities to notify the Secretary immediately.²⁸ HHS’s final rule interprets “immediately” to mean concurrently with the notification sent to individuals (*i.e.*, no later than 60 calendar days following discovery of a breach).²⁹ For breaches involving less than 500 individuals, which must be documented in a log submitted annually to the Secretary, the HHS Rule designates a submission date: no later than 60 days after the end of each calendar year.³⁰

E. Business Associates

HHS encourages covered entities to address the timing of breach notifications in their business associate contracts, as discovery of a breach by a business associate may be imputed to a covered entity (and start the clock for notifying customers) if the business associate is deemed an agent of the covered entity under federal common law. In a slight departure from the statutory language, the HHS Rule requires that, when notifying the covered entity about a breach, the business associate must include identification of the affected individuals only “to the extent possible.”³¹ The business associate can provide additional information after the initial notification.

²⁴ *Id.* at 42,768.

²⁵ Workforce member, as defined in HIPAA, means employees, volunteers, trainees, and other persons whose conduct is under the direct control of such entity. 45 C.F.R. § 160.103.

²⁶ 74 Fed. Reg. at 42,768.

²⁷ *Id.*

²⁸ HITECH Act, § 13402.

²⁹ 74 Fed. Reg. at 42,768-69.

³⁰ *Id.* at 42,769.

³¹ *Id.*

F. Preemption

Under the HIPAA statute, federal requirements will supersede any contrary provisions of state law.³² Although the HIPAA Privacy Rule contains an exception to preemption for more stringent State privacy laws,³³ HHS does not believe this exception applies to the breach notification regulations.³⁴ Thus, according to HHS, the breach notification requirements will preempt contrary state laws, even more stringent ones. In general, however, HHS believes that covered entities can comply with both the regulations and applicable state laws, and, in most cases, a single notification will be sufficient.³⁵ HHS is soliciting comments on this issue.

G. Updated Guidance

Along with the rule, HHS issued an update to its guidance on technologies and methodologies to secure PHI for purposes of the breach notification provisions. In this guidance, after considering public comment, HHS clarified that covered entities and business associates should store decryption tools on a device or at a location separate from the data they are used to encrypt or decrypt.³⁶

H. Opportunity for Comment

HHS will be accepting comments on the HHS Rule through October 23, 2009. In particular, HHS is soliciting comments on the issue of preemption and the interaction between the rule and state breach notification laws and on the limited data set exception under the breach definition. Comments on the information collection requirements associated with the HHS Rule will be accepted through September 8, 2009.

III. FTC BREACH NOTIFICATION RULE

The HITECH Act provides the FTC with the authority to issue and enforce temporary³⁷ breach notification requirements applicable to vendors of PHR, PHR related entities, and third party services providers.³⁸ Under the Act, vendors of PHR and PHR related entities must notify customers of any breach of unsecured PHR identifiable information.³⁹ Third party service providers must similarly notify such vendors or entities.⁴⁰ The FTC issued a notice of proposed rulemaking to implement these provisions on April 20, 2009.⁴¹ Notable aspects of the final FTC Rule are discussed below.

³² 42 U.S.C. § 1320d-7.

³³ 45 C.F.R. § 160.203.

³⁴ 74 Fed. Reg. at 42,756. HHS states that the preemption exceptions apply only to the provisions of the Privacy Rule promulgated under Section 264(c) of the HIPAA statute.

³⁵ The FTC takes a slightly different approach to preemption, finding that HIPAA's "contrary" standard will not preempt state laws imposing additional breach notification requirements. Content requirements may be different under state law; for example, some state laws require that notices contain contact information for consumer reporting agencies or advice on monitoring credit reports. However, the FTC believes that entities can comply with both federal and state requirements by setting forth all of the information required in a single breach notice.

³⁶ *Id.* at 42,742.

³⁷ The HITECH Act provides that the FTC has authority to issue and enforce temporary breach notification rules until Congress enacts new legislation implementing recommendations in a joint HHS/FTC study regarding vendors of PHR and related entities. HITECH Act, § 13424. Violations of rules will be treated as an unfair or deceptive trade practice in violation of the FTC Act.

³⁸ HITECH Act, § 13407.

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ Proposed Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009). To access a previous Covington E-Alert about the proposed FTC breach notification rule, [click here](#).

A. Unauthorized Acquisition of Data

For FTC-regulated entities, the HITECH Act defines a breach of security as “the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the authorization of the individual.”⁴² In many instances, it will be fairly easy to determine whether unsecured PHR identifiable health information has been acquired without authorization. In other cases, there may be unauthorized access to data, but it will be unclear, without further investigation, whether the data has also been acquired. To address the difficulty of determining whether *access* to data did or did not lead to *acquisition*, the final rule creates a presumption that unauthorized persons have acquired information if they have access to it.⁴³ This presumption can be rebutted with reliable evidence. Unauthorized acquisition, therefore, is significantly different under the FTC and HHS Rules, as HHS defines the term as an impermissible use or disclosure under the HIPAA Privacy Rule.

B. PHR Identifiable Health Information

Based on comments received, the FTC confirmed that de-identified data under HIPAA will not be considered PHR identifiable health information. However, the FTC declined to adopt a blanket statement that limited data sets under HIPAA are not PHR identifiable health information, finding that the risk of re-identification is too high.

C. Third Party Service Providers

The FTC Rule specifies that third party service providers must, in the event of a breach, provide notice to an official designated in a written contract by the PHR vendor or related entity to receive such notices, or, if no designation is made, to a senior official at the PHR vendor or related entity.⁴⁴ The service provider must obtain acknowledgment that notice was received.⁴⁵ To avoid situations where a third party service provider may be unaware that it is dealing with a PHR vendor (*e.g.*, cloud computing service providers), the FTC Rule requires PHR vendors and related entities to notify service providers of their status as PHR vendors and related entities subject to the FTC breach notification rule.⁴⁶ The agency clarified that the FTC Rule requires a service provider to identify to the PHR vendor or related entity only customers whose information was breached (as opposed to all individuals affected by a breach).

D. Notification to Individuals

The FTC Rule provides that an individual must be given notice by first-class mail or by e-mail, if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail and does not exercise that choice.⁴⁷ In cases where there is insufficient contact information for 10 or more individuals affected by a breach, the HITECH Act requires provision of a substitute form of notice through a conspicuous posting on the home page of the entity's Web site or through the media.⁴⁸ The FTC Rule

⁴² HITECH Act, § 13407.

⁴³ 74 Fed. Reg. at 42,980.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.* at 42,980-81.

⁴⁷ *Id.* at 42,981. The proposed rule required express affirmative consent for e-mail notice, but numerous commenters convinced the FTC that, because the relationships contemplated among the PHR vendors, related entities, and consumers take place entirely online, e-mail notice is an appropriate default option.

⁴⁸ HITECH Act, § 13407.

shortened the time period for the Web site posting from the 6-month period in the proposed rule to 90 days.⁴⁹

E. Notification to FTC

The FTC Rule requires PHR vendors and related entities to notify the FTC following a breach of security.⁵⁰ For breaches involving 500 or more individuals, this notice must be provided as soon as possible and in no case later than *10 business days* after the breach is discovered.⁵¹ Like the HHS Rule, the FTC Rule provides that, for breaches involving fewer than 500 individuals, the PHR vendor or related entities may maintain a log that is to be submitted annually to the FTC no later than 60 days following the end of the calendar year.⁵²

If you have any questions concerning the material discussed in this client alert, please contact the following members of our health care and privacy practice groups:

Anna Kraus	202.662.5320	akraus@cov.com
Demetrios Kouzoukas	202.662.5057	dkouzoukas@cov.com
Rachel Grunberger	202.662.5033	rgrunberger@cov.com

This information is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP is one of the world's preeminent law firms known for handling sensitive and important client matters. This promotional communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts. Covington & Burling LLP is located at 1201 Pennsylvania Avenue, NW, Washington, DC 20004-2401.

© 2009 Covington & Burling LLP. All rights reserved.

⁴⁹ 74 Fed. Reg. at 42,981.

⁵⁰ *Id.*

⁵¹ *Id.* The ten-day period is more generous than the FTC's proposed rule, which imposed a five-day notice requirement, but differs from the HHS Rule, which specifies that notice is to be provided to the Secretary within 60 days of the individual notice.

⁵² *Id.*