



HEALTHCARE PRIVACY UPDATE

The Information Law and Privacy Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyberlaw. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property and white collar lawyers. We frequently advise regarding HIPAA and Healthcare Privacy issues.

For more information, please contact:

Alan Charles Raul
+1.202.736.8477
araul@sidley.com

Healthcare Practice

Our Healthcare Practice represents participants in all facets of the healthcare industry, including pharmaceutical, biotech and device companies, DME suppliers, hospitals, skilled nursing facilities, physician-owned companies, professional associations and research institutions. Our lawyers combine a strong background in the complexities of healthcare financing and delivery, including coding, reimbursement, and coverage issues, privacy and security, trade regulation and competition.

For further information, please contact:

Paul E. Kalb, M.D.
+1.202.736.8050
pkalb@sidley.com

This **Sidley Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.

HHS and FTC Issue Rulemakings on HITECH Breach Notification Provisions

The U.S. Department of Health and Human Services (“HHS”) and Federal Trade Commission (“FTC”) recently issued separate rules implementing the groundbreaking breach notification provisions of the Health Information Technology for Economic and Clinical Health Act (“HITECH”). HHS’ breach notification interim final rule applies to entities that meet the definition of “covered entity” or “business associate” under the privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). FTC’s breach notification final rule applies to entities – other than covered entities or business associates – that offer or maintain personal health records (“PHR vendors”), certain entities offering products or services through PHR Web sites or providing services to PHR vendors, and third-party service providers of such entities.¹

Although HHS and FTC each stated that they consulted closely to harmonize the two rules, the agencies’ regulations contain at least two major differences. Under the HHS interim final rule, a reportable breach occurs only if there is a significant risk of harm to the individual. In contrast, the FTC final rule presumes unauthorized acquisition when there is unauthorized access to data unless the entity that discovers the incident can rebut the presumption with “reliable evidence” showing there has not been, or could not reasonably have been, unauthorized acquisition of such data. Additionally, the HHS interim final rule applies to protected health information (“PHI”) in any form (paper or electronic) whereas the FTC rule applies only to electronic information.

The HHS and FTC rules take effect 30 days after publication in the Federal Register (September 23, 2009, for the HHS interim final rule with request for comments, and September 24, 2009, for the FTC final rule). Significantly, however, HHS and FTC have stated that they will not enforce the notification requirements for breaches that are discovered within 180 days from the date of publication in the Federal Register (February 22, 2010). Comments on the HHS interim final rule are due October 23, 2009.

1. HHS' Breach Notification Interim Final Rule²

- **Entities Covered by the Interim Final Rule:** HIPAA covered entities (*e.g.*, healthcare providers, healthcare clearinghouses, and health plans) and their business associates.
- **Covered Data:** Unsecured Protected Health Information.
- **Excluded Data:** Data secured through the technologies and methodologies specified by HHS and data that removes date of birth, zip code, and the 16 identifiers that must be removed to satisfy the definition of a limited data set.
- **Definition of Breach:** The acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. The definition of breach excludes: (i) unintentional and inadvertent uses and disclosures of PHI by workforce members or others acting under the authority of a covered entity or business associate where, among other requirements, the PHI is not further used or disclosed in violation of the Privacy Rule; and (ii) unauthorized disclosures of PHI where the covered entity or business associate has a good faith belief that the person receiving the information could not reasonably have retained it.
- **Standard for Determining Breach:** Whether the incident poses a significant risk of financial, reputational, or other harm to the affected individual.
- **Time Frame for Notification:** Without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- **Required Notifications Include:** Notifications of breaches must be made to affected individuals and the HHS Secretary. In cases where the breach affects 500 or more residents of a particular State or jurisdiction, prominent media outlets must also be notified.
- **Effective Date:** September 23, 2009.
- **Date Enforcement Begins:** February 22, 2010.

Section 13402 of HITECH requires HIPAA-covered entities to provide notification to affected individuals, the Secretary of HHS, and, in some cases, the media following the discovery of a “breach” of “unsecured PHI.”³ Additionally, upon discovery of a breach, HITECH requires business associates to notify the affected covered entity, so that the covered entity may notify its patients or enrollees.

A. *Three-Part Test for Determining if a “Breach” Has Occurred*

HITECH defines a “breach” as “the unauthorized acquisition, access, use, or disclosure of [PHI] which compromises the security or privacy of such information.”⁴ In the preamble to the interim final rule, HHS sets forth a three-part test for determining when the statutory standard for breach has been met.

Under the first prong of the three-part test, the covered entity or business associate must determine if there has been a use or disclosure of unsecured PHI in violation of the Privacy Rule. Those disclosures or uses that are permissible under the Privacy Rule, such as a disclosure of PHI that is incident to an otherwise permissible use or disclosure, do not qualify as a potential breach.

Second, if there has been a use or disclosure of unsecured PHI in violation of the Privacy Rule, the covered entity or business associate must next determine whether the impermissible use or disclosure “compromises the security or privacy of the [PHI].” For an unauthorized use or disclosure to “compromise the security or privacy of the [PHI],” the impermissible access or disclosure must “pose a significant risk of financial, reputational, or other harm to the individual.” Covered entities and business associates who discover a potential breach must perform a documented risk assessment to determine if a “significant risk” of harm has occurred.

As an example, HHS stated that, if a covered entity impermissibly discloses the type of services the individual received (*e.g.*, by disclosing the name of the individual and a specialized health facility from which the individual received services) or the PHI disclosed includes information that

increases the risk of identity theft (*e.g.*, disclosure of a social security number or credit card information), the impermissible disclosure would likely cause a significant risk of financial, reputational, or other harm to the individual. In contrast, HHS explained that if a covered entity improperly uses or discloses PHI that merely included the name of an individual and the fact that he or she received unspecified services from a general hospital, such disclosure would not constitute a significant risk of financial or reputational harm to the individual and thus would not constitute a “breach.”

Third, if the impermissible use or disclosure compromises the privacy or security of the PHI, the covered entity or business associate must next determine whether the incident falls under an applicable exception such that an authorized use or disclosure would not constitute a breach. The interim final rule’s exceptions generally mirror the three statutory exceptions with certain slight modifications. Broadly speaking, the first two exceptions cover unintentional and inadvertent uses and disclosures of PHI by workforce members or others acting under the authority of a covered entity or business associate where, among other requirements, the PHI is not further used or disclosed in violation of the Privacy Rule. The third exception covers unauthorized disclosures of PHI where the covered entity or business associate has a good faith belief that the person receiving the information could not reasonably have retained it. This would be the case, for example, where a health plan sends Explanation of Benefits (“EOBs”) to the wrong addresses, but the EOBs are returned to the sender without having been opened.

B. Discovery and Time Frame for Notification of a Breach

Largely consistent with the statutory language, the interim final rule provides that breaches are treated as discovered by a covered entity “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 [or] . . . any person, other than the person committing the breach, who is a workforce member or agent of the covered entity . . .” A breach is treated

as having occurred at the time when the incident becomes known, not when the covered entity or business associate concludes its analysis of whether the facts constitute a breach. The interim final rule specifies that the federal common law of agency applies to the determination of who is an agent of the covered entity. In those instances where a business associate is acting as an agent of a covered entity, as opposed to an independent contractor, the business associate’s discovery of a breach will be imputed to the covered entity. Significantly, in such cases, the covered entity would need to provide the required notifications from the time the business associate discovers the breach, not from the time the business associate notifies the covered entity.

Upon the discovery of a breach, covered entities and business associates must provide the required notifications “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach” unless a narrow exception for law enforcement activities applies. HHS clarified that 60 days is the outer limit for fulfilling the breach notification requirements, and that, depending on the facts and circumstances, it may be unreasonable to wait until the 60th day to provide notification.

Consistent with section 13402(d)(2) of HITECH, the interim final rule provides that, following an impermissible use or disclosure under the Privacy Rule of unsecured PHI, covered entities and business associates have the burden of demonstrating that all notifications were made as required by the interim final rule. HHS made conforming changes to the HIPAA Enforcement Rule to make clear that, during any administrative hearing, the covered entity has the burden of going forward and the burden of persuasion with respect to these issues. Covered entities and business associates are liable for failing to provide notice of a breach when the covered entity or business associate did not know, but by exercising reasonable diligence should have known, of a breach. For that reason, it is critical that covered entities and business associates should develop reasonable relevant personnel regarding the requirements of the interim final rule.

C. *Required Notifications*

1. Notice to Individuals

Under HHS' interim final rule, covered entities must provide written notice to the individual, or substitute notice if contact information is insufficient or out-of-date. For example, if the covered entity learns that the home address it has for a patient is out-of-date but it has the patient's e-mail address, it may provide substitute notice by e-mail even if the patient has not agreed to electronic notice. If a covered entity has insufficient or out-of-date contact information for 10 or more individuals, then the rule requires the covered entity to provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In addition, substitute notice through the Web site or media for 10 or more individuals requires the covered entity to have a toll-free number, active for 90 days, where an individual can learn about the breach. In addition, covered entities may also provide notice by telephone or other means if there is an urgent need to provide notice because of possible imminent misuse of PHI.

2. Notice to the Media and the HHS Secretary

The HHS interim final rule also requires that notice be provided to prominent media outlets serving a State or jurisdiction (an area smaller than a State such as a county, city or town) following the discovery of a breach if the covered entity determines, or reasonably believes, that the unsecured PHI of 500 or more residents of such State or jurisdiction is accessed, acquired or disclosed. Breaches involving residents of multiple States or jurisdictions do not have to be reported to the media unless 500 or more individuals of any one State or jurisdiction are affected.

Covered entities must also notify the HHS Secretary of breaches of unsecured PHI involving 500 or more individuals. Notification of the Secretary is required regardless of whether the affected individuals reside in one or more States or jurisdictions. For breaches of unsecured PHI involving fewer than 500 individuals, a covered entity must maintain a log or

other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notification for breaches occurring during the preceding calendar year, in the form specified by the Secretary on the HHS Web site.

D. *Safe Harbor for Secured PHI*

As part of the interim final rule, HHS updated its guidance specifying certain encryption and destruction methodologies approved by the National Institute of Standards and Technology ("NIST") as the methodologies and technologies that render PHI, as well as the PHR identifiable health information,⁵ unusable, unreadable, and indecipherable to unauthorized individuals. Although covered entities and business associates are not required to use encryption and destruction methodologies, those that do so in accordance with the HHS guidance should fall within the safe harbor for secure PHI and will not be subject to the potentially onerous breach notification requirements discussed above.

Significantly, HHS declined to adopt a blanket rule that the use of a limited data set renders PHI secure due to the potential risk of re-identification of this information. HHS instead adopted a narrow exclusion to the definition of breach for PHI that omits the 16 direct identifiers set forth in 45 C.F.R. § 164.514(e)(2), date of birth, and zip code. Thus, breach of such data sets is not considered a reportable breach.

2. FTC's Breach Notification Final Rule⁶

- **Entities Covered by the Final Rule:** PHR vendors, PHR related entities, and third party service providers.
- **Covered Data:** Unsecured PHR identifiable health information.
- **Excluded Data:** Data in a PHR that is secured through the technologies and methodologies specified by HHS.
- **Definition of Breach:** The acquisition of unsecured PHR identifiable health information without the individual's authorization.
- **Standard for Determining Breach:** Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the PHR vendor, PHR related entity, or third party service provider has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.
- **Time Frame for Notification:** Without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- **Required Notifications Include:** Notifications of breaches must be made to affected individuals and the FTC. In cases where the breach affects 500 or more residents of a particular State or jurisdiction, prominent media outlets must also be notified.
- **Effective Date:** September 24, 2009.
- **Date Enforcement Begins:** February 22, 2010.

The FTC's final rule applies to PHR vendors and PHR related entities – entities that historically have not been directly subject to the Privacy Rule. Those PHRs that are offered or sponsored by a covered entity are subject to the Privacy Rule and therefore, are subject to the HHS breach notification provisions. Vendors with a dual role as a business associate offering PHRs to a covered entity's patients or enrollees and a PHR vendor to the public would be subject to both HHS' and FTC's breach notification requirements. Significantly, however, the FTC will deem compliance with HHS breach notification requirements as compliance with the FTC rule where a PHR vendor serving in a dual role provides notice to individuals on behalf of a HIPAA-covered entity and meets certain other requirements. FTC's approach ensures that consumers do not receive more than one breach notification for a single breach.

Similar to the HHS interim final rule, the FTC final rule requires PHR vendors and "PHR related entities" (entities that offer products or services through the Web sites of PHR vendors or covered entities that offer PHRs, or entities that access information in a PHR or send information to a PHR) to provide notification to affected individuals, the FTC, and, in certain cases, the media following the discovery of a "breach" of unsecured "PHR identifiable health information." PHR related entities include entities that advertise or offer certain services through a PHR vendor's Web site, such as a Web-based application that helps consumers manage their medications, a Web site offering an online personalized health checklist, and a "brick-and-mortar" company advertising dietary supplements online. Search engines are PHR related entities if they appear on PHR vendor Web sites.

Finally, the rule requires "third party service providers" of PHR vendors and PHR related entities to notify a designated official of the PHR vendor or PHR related entity of breaches. Third party service providers include, for example, entities that provide billing, debt collection or data storage services to PHR vendors or PHR related entities.

A. Failure to Define Clearly PHR

The FTC defines PHR as “an electronic health 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.” Given the breadth and lack of clarity of the definition of PHR, many entities, such as pharmaceutical manufacturers that offer health tracker tools or other Web portals that allow consumers to input and store health-related data on their Web site, may be subject to the FTC’s breach notification final rule.

B. Breach Notification Requirements

The FTC’s final rule mandates certain notification requirements in the event of a “breach of security” of unsecured PHR identifiable health information. The final rule defines “breach of security” as “the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual.” According to the FTC, an entity’s use of information to enhance individuals’ experience with their PHRs would be within the scope of the individual’s authorization, provided such use is consistent with the entity’s disclosures and individuals’ reasonable expectations.

C. Discovery and Time Frame for Notification of a Breach

There are a number of similarities between the HHS interim final rule and FTC final rule with respect to discovery and the timeframe for notification of a breach. Like the HHS interim final rule, the FTC final rule requires PHR vendors and related entities to provide the required notifications “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of security” unless a narrow exception for law enforcement activities applies. FTC explicitly states that a covered entity “need not establish all prerequisites for triggering breach notification before the 60 day time period starts.” The purpose of the 60 day period is to give entities time to conduct an investigation; the time period does not start when the investigation is complete. Similar to the HHS interim final rule, the FTC final rule mandates that

discoveries by third party service providers be imputed to the PHR vendor or related entity if the third party service provider is an agent of that entity. The FTC final rule also requires individual notice and notice to the FTC, as well as notice to the media under certain circumstances.

D. De-Identified Data and Limited Data Sets

The FTC confirmed that data that is de-identified in accordance with the Privacy Rule would not constitute “PHR identifiable health information” due to the low risk that such data will be re-identified by unauthorized third parties. Thus, if such information is breached, it would not trigger any notice requirements.

Like HHS, the FTC declined to adopt a blanket exception for limited data sets because FTC believes the risk of re-identification is too high. Unlike HHS, however, the FTC did not create a narrow safe harbor for health information that excludes birth date and zip code, in addition to the 16 identifiers listed in 45 C.F.R. § 164.514(e)(2). Instead, FTC stated that, consistent with the rebuttable presumption standard described above, “entities still may be able to show, in specific instances, that there is no reasonable basis to identify individuals whose data has been breached, and thus no need to send breach notices.”

★ ★ ★ ★

Organizations that handle PHI, create or offer PHRs, or offer services in connection with PHRs should evaluate the implications of the HHS interim final rule and FTC final rule. We would be pleased to assist clients with any questions or concerns or the preparation of comments to the HHS interim final rule.

Anna L. Spencer
aspencer@sidley.com
+1.202.736.8445

Eileen L. Kahaner
ekahaner@sidley.com
+1.415.772.7432

Alan Charles Raul
araul@sidley.com
+1.202.736.8477

Meenakshi Datta
mdatta@sidley.com
+1.312.853.7169

Deitzah Woll
dwill@sidley.com
+1.312.853.3456

Endnotes

- ¹ Sidley Austin LLP released related updates on February 19, 2009 (describing the key privacy and security provisions of HITECH), and April 27, 2009 (describing the HHS guidance regarding the methods and technologies that render PHI secure and the FTC proposed rule regarding breach notification). These updates are available at <http://www.sidley.com/sidleyupdates/Detail.aspx?news=3932> and <http://www.sidley.com/sidleyupdates/Detail.aspx?news=4003>.
- ² To implement the HITECH breach notification provisions, HHS created a new Subpart D of Part 164 of the Code of Federal Regulations.
- ³ Under the new regulations, “unsecured PHI” is defined as “[PHI] that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary” The guidance developed by the Secretary of HHS is discussed in Section 1.D of this update.
- ⁴ HITECH Act, § 13400(1).
- ⁵ PHR identifiable health information is defined as “‘individually identifiable health information,’ as defined in section 1171(6) of the Social Security Act[], and, with respect to an individual, information: (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.” Entities subject to the FTC final rule, such as PHR vendors and related entities, that employ encryption and destruction in conformity with HHS’ guidance will not be required to provide the specified notifications.
- ⁶ The FTC’s breach notification requirements are temporary to the extent that Congress enacts future legislation that would apply new notification requirements to entities that are subject to the rule.

To receive future copies of Healthcare Privacy Practice Updates via email, please send your name, company or firm name and email address to Lacy Quarles at lquarles@sidley.com.

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm’s offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.

SIDLEY AUSTIN LLP
SIDLEY