

Mintz, Levin, Cohn, Ferris,
Glovsky and Popeo, P.C.

An Overview of the Impact of the American Recovery and Reinvestment Act of 2009 on the HIPAA Medical Privacy and Security Rules

Alden J. Bianchi

Updated as of: October 3, 2009

**An Overview of the Impact of the American Recovery and
Reinvestment Act of 2009 on the HIPAA Medical Privacy and Security
Rules**

TABLE OF CONTENTS

	<u>PAGE</u>
I. Background	2
A. <i>The Privacy Rule</i>	2
B. <i>The Security Rule</i>	2
C. <i>Business Associates</i>	3
D. <i>The American Reinvestment and Recovery Act</i>	3
II. Summary of the HITECH Changes	3
A. <i>Definition of “Breach”</i>	4
B. <i>Expanded Privacy and Security Provisions</i>	4
C. <i>Notification in the Case of Breach</i>	7
1. Breaches Relating to Unsecured PHI	7
2. Breaches of	14
D. <i>Revisions to the “Minimum Necessary” Standard</i>	16
E. <i>Restrictions on Sales of PHI</i>	17
F. <i>Patient Access to and Restrictions on PHI</i>	17
G. <i>Marketing</i>	18
H. <i>Enforcement</i>	19
III. Conclusion	20

An Overview of the Impact of the American Recovery and Reinvestment Act of 2009 on the HIPAA Medical Privacy and Security Rules

Alden J. Bianchi, Esq. *

I. Background

The administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996¹ (“HIPAA”) established a comprehensive set of rules regulating, among other things, to the privacy and security of medical information. HIPAA itself contained no substantive privacy rules. Instead, Congress set itself a three-year deadline to enact health information privacy legislation. If, as turned out to be the case, lawmakers were unable to pass such legislation before the deadline, the Secretary of the U.S. Department of Health and Human Services (“HHS”) was instructed to promulgate regulations on Congress’ behalf. The HIPAA privacy rule² established a set of patient rights, including the right of access to one’s medical information, and placed certain limitations on when and how health plans and health care providers may use and disclose such protected health information (“PHI”).

A. The Privacy Rule

The HIPAA privacy regulations prescribe detailed rules governing the conduct of “covered entities.”³ Covered entities include (i) health care providers, (ii) health care clearinghouses and (iii) health plans—including employer-sponsored group health plans. Generally, plans and providers may use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual’s authorization and with few restrictions. In certain other circumstances (e.g., disclosures to family members and friends), the rule requires plans and providers to give the individual the opportunity to object to the disclosure. The rule also permits the use and disclosure of health information without the individual’s permission for various specified activities (e.g., public health oversight, law enforcement) that are not directly connected to the treatment of the individual. For all uses and disclosures of health information that are not otherwise required or permitted by the rule, plans and providers must obtain a patient’s written authorization.

B. The Security Rule

* Alden J. Bianchi is a Member in the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., Boston, Massachusetts. © 2009 Alden J. Bianchi, Esq., all rights reserved.

¹ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 2021-2031.

² 45 C.F.R. §§ 160, 164 (2008).

³ *Id.* § 160.103.

In addition to health information privacy standards, HIPAA's Administrative Simplification provisions instructed the Secretary to issue security standards to safeguard PHI in electronic form against unauthorized access, use, and disclosure.⁴ The security rule⁵ specifies a series of administrative, technical, and physical security procedures for providers and plans to use to ensure the confidentiality of electronic health information.

C. *Business Associates*

The HIPAA privacy and security rules also permit covered entities to share health information with their "business associates" who provide a wide variety of functions for them, including legal, actuarial, accounting, data aggregation, management, administrative, accreditation, and financial services.⁶ A covered entity is permitted to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will appropriately safeguard the information. Importantly, however, because the privacy and security rules govern covered entities, neither rule imposes any substantive requirements directly on business associates. Therefore, prior to HITECH, violations of the HIPAA privacy and security rules could not be enforced directly against business associates.

D. *The American Reinvestment and Recovery Act*

The recently enacted American Reinvestment and Recovery Act⁷ ("ARRA") makes business associates directly responsible for complying with HIPAA privacy and security rules, provides for increase enforcement activity, and imposes penalties for noncompliance. Also included are new breach notification requirements and new substantive privacy rights. These provisions are contained in ARRA Title XIII, which is referred to as the "Health Information Technology for Economic and Clinical Health" (or "HITECH") Act. Many of the changes have delayed effective dates, but some are effective now. This paper explains the key features of the HITECH provisions of the ARRA.

Prior to ARRA, HIPAA imposed privacy and security requirements only on covered entities. Business associates (e.g., third-party administrators, consultants, and other vendors) were not directly covered by the HIPAA rules, but they were indirectly regulated through business associate agreements with covered entities. Now, certain HIPAA provisions and penalties will apply to business associates directly.

HITECH is generally effective as of February 17, 2009, although most of the substantive HITECH provisions have delayed effective dates.⁸

II. **Summary of the HITECH Changes**

⁴ 42 U.S.C. § 1320d-2(d) (2000).

⁵ 45 C.F.R. § 160, 164.

⁶ *Id.* § 164.308(b).

⁷ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 [hereinafter ARRA].

⁸ ARRA § 13423.

The key changes to the HIPAA privacy and security rule under the HITECH act are as follows:

A. *Definition of “Breach”*

For the most part, HITECH adopts the definitions established by the HIPAA privacy and security rules for such terms as business associate, covered entity, electronic health record, electronic medical record, health care operations, health care provider, health plan, National Coordinator, payment, personal health record, protected health information, Secretary, security, state, treatment, use, and vendor of personal health records.⁹ The existing rules define the term “disclosure” to mean, simply, “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.”¹⁰

HITECH introduces the term “breach.”¹¹ It also makes clear that certain inadvertent disclosures can constitute a “breach” for various purposes. Under HITECH, unauthorized “disclosures” generally result in a breach. But a disclosure where a person would not reasonably be able to retain the information disclosed is not a breach. Also not a breach is any inadvertent disclosure from an individual otherwise authorized to access PHI to another similarly situated individual, provided that such information is not further “acquired, accessed, used, or disclosed” other than in accordance with the requirement of the privacy rule.¹²

B. *Expanded Privacy and Security Provisions*

HITECH generally expands the reach of the HIPAA privacy and security provisions and their accompanying penalties, to business associates. With respect to the security requirements, ARRA § 13401(a) is clear:

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity. (Emphasis added.)

45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 establish rules requiring the adoption of administrative, physical, and technical safeguards and implementation of reasonable and appropriate policies and procedures. (Administrative safeguards are intended to address the organization of the internal security infrastructure of a covered entity or business associate; physical safeguards are intended to protect electronic

⁹ *Id.* § 13400.

¹⁰ 45 C.F.R. 164.103.

¹¹ *Id.* § 13400(1).

¹² *Id.* § 13400(1)(B)(iii).

systems and data from threats, environmental hazards, and unauthorized access; and technical safeguards are primarily IT functions used to protect and control access to data.) As a result, a business associate is obligated to comply with the requirements of the HIPAA security rule in the same way and to the same extent as a covered entity. This will require business associates to, among other things, conduct a formal risk assessment, appoint a security officer, adopt written security policies and procedures, and train their employees. They will also need to implement safeguards to protect electronic PHI (or “ePHI”), such as encrypting emails and computer files and limiting access to records. These obligations will also be required to be included in business associate agreements.

The extent to which business associates must comply with the requirements of the HIPAA privacy rule is not as clear. ARRA § 13404(a) reads:

In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity. (Emphasis added.)

45 C.F.R. § 164.504(e) is the business associate requirement. The substantive requirements of the HIPAA privacy rule are set out in 45 C.F.R. § 164.512, to which HITECH makes no reference. Thus, while business associates are now bound by the requirement to enter into a business associate agreement, it is not clear to what extent they must comply with the substance of each particular privacy requirement. The statute clearly requires that business associates use and disclose PHI in accordance with the business associate agreement requirements, and it also makes business associates subject to additional privacy requirements added by HITECH.¹³ If, for example, a business associate knows of a material breach by a covered entity, the business associate is required to take action to cure the breach or end the violation. If a cure is not possible, the business associate must terminate the agreement, and if neither cure nor termination is possible, the business associate must report the breach to HHS.

The Conference Committee report accompanying ARRA includes the following statement as to the legislators’ intent:

The House bill would apply the HIPAA Privacy Rule, the additional privacy requirements, and the civil and criminal penalties for violating

¹³ *Id.* § 13404(a).

those standards to business associates *in the same manner as they apply to the providers and health plans for whom they are working.*¹⁴

Some clues to understanding how the HIPAA privacy rule should be applied to business associates are found in a transcript of a February 25, 2009 meeting of the Department of Health and Human Services, National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality and Security,¹⁵ which includes the following statement by Susan McAndrew, an attorney with the HHS Office for Civil Rights:

I will skip over, if I could, to the counterpart of this provision which is on Page 3, 13404, which essentially does the same thing [i.e., extends the substantive provisions of the security rule] with respect to privacy, although it does it in a much less elegant manner than the security rule. Provisions were extended to business associates, but this will essentially make business associates liable for privacy violations in the same way that covered entities are today responsible for privacy violations. *Right now the interpretation is this will probably be violations with regard to the use and disclosure of information. These provisions do not in effect, as is sometimes characterized, turn business associates into covered entities. It does not do that. And business associates are not required to take on the panoply of all the administrative requirements that we impose on covered entities and can hold covered entities liable for violating.* They are very specific on the security side, unfortunately less specific on the privacy side, as to what the standard is that business associates will now be held to and liable for. But clearly uses and disclosures of information in violation of the privacy rule will be a liability directly on business associates.¹⁶

The committee then goes on to discuss what impact the change will have on business associates, particularly in light of the statement in the Conference Committee report that “this will essentially make business associates liable for privacy violations in the same way that covered entities are today responsible for privacy violations.”¹⁷ The tone and tenor of the discussion indicate the regulators will want to read the new rules expansively.

Depending on how the regulators resolve this issue, business associates might be required to comply with many or even all of the substantive HIPAA privacy provisions. This would require business associates to adopt privacy policies and procedures, appoint a privacy official, train their workforces, etc. At a minimum, however, they will be subject to the business associate agreement requirement, the new privacy and security

¹⁴ H.R. Rep. No. 111-16, at 493 (2009) (Conf. Rep.) (emphasis added).

¹⁵ Dep’t of Health and Human Services, Nat’l Comm. on Vital and Health Statistics Subcomm. on Privacy, Confidentiality and Security Meeting Transcript (Feb. 25, 2009), *available at* <http://www.ncvhs.hhs.gov/090225t1.htm>.

¹⁶ *Id.* (emphasis added).

¹⁷ *Id.*

mandates and the HIPAA civil and criminal penalties in the same manner as covered entities.

HITECH's business associate provisions take effect one year from the enactment of ARRA, or February 17, 2009.

C. *Notification in the Case of Breach*

Nothing the in the HIPAA privacy or security rules require covered entities, or anyone else, to notify the government or individuals of a breach involving the privacy, security, or integrity of protected health information. Covered entities are instead bound by an obligation to mitigate any harm caused by a breach,¹⁸ which may include in appropriate instances documenting the breach and changing internal policies.

HITECH includes two sets of rules imposing notice requirements in the case of a breach. The first governs covered entities and business associates, and it regulates breaches of "unsecured protected health information."¹⁹ The second governs vendors of "Personal Health Records" ("PHRs") and other non-HIPAA-covered entities.²⁰ This latter rule regulates breaches of unsecured personal health records. HHS is charged with issuing guidance specifying the technologies and methodologies that would render both PHI and PHRs "unusable, unreadable, or indecipherable" to unauthorized individuals.²¹ The Federal Trade Commission (or "FTC") is directed to issue rules requiring vendors of personal health records and related entities to notify individuals in the event of a breach relating to their personal health records.²²

1. Breaches Relating to Unsecured PHI

HITECH imposes new notice requirements on covered entities and business associates in the event of a "breach" of unsecured PHI. Covered entities must generally notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach. Where a breach is discovered by a business associate, the business associate is required to notify the covered entity. There are exceptions to the breach notification requirement for unintentional acquisition, access, use or disclosure of protected health information.²³

The statute defines term "breach" for this purpose is defined as the unauthorized acquisition, access, use or disclosure of PHI that compromises the privacy or security of that information, excluding certain unintentional or inadvertent disclosures involving the "acquisition, access, use or disclosure of protected health information,"²⁴ but only if the disclosure is to an individual authorized to access health information at the same facility. "Unsecured PHI" is PHI that is not secured through use of a technology or methodology

¹⁸ 42 C.F.R. § 164.530(f).

¹⁹ ARRA § 13402.

²⁰ *Id.* § 13407.

²¹ *Id.* § 13402(h)(2).

²² *Id.* § 13407(g)(1).

²³ *Id.* § 13402.

²⁴ *Id.* § 13400(1)(A).

identified by HHS as rendering the information unusable, unreadable or indecipherable to unauthorized persons.²⁵

Notice of a breach must be provided without unreasonable delay and within 60 days after “discovery.” A breach is “discovered” as of the first day that it is known (or reasonably should have been known) to the covered entity or the business associate. (A business associate that discovers a breach is required to notify the covered entity.) A covered entity or business associate is treated as having knowledge of a breach on the day that any employee, officer or other agent has such knowledge (except for the individual who committed the breach). The Notice of breach must, at a minimum, contain (i) a brief description of the breach, including dates, (ii) a description of types of unsecured PHI involved, (iii) the steps the individual should take to protect against potential harm, (iv) a brief description of steps the covered entity or business associate has taken to investigate the incident, mitigate harm and protect against further breaches, and (v) contact information.

ARRA requires HHS to issue interim final regulations no later than August 16, 2009, and HITECH’s breach notice requirements as they apply to HIPAA covered entities and business associates will apply to breaches discovered on or after 30 days following date regulations.²⁶

(a) *The April 17, 2009 Encryption Guidance*

On April 17, 2009, HHS issued a proposed rule specifying how entities may safeguard PHI and PHRs so as to render each “unusable, unreadable, or indecipherable to unauthorized individuals,”²⁷ thereby exempting entities from the HITECH breach notification requirements. The proposed rule was developed by HHS with assistance from the Office of the National Coordinator for Health Information Technology, and the Centers for Medicare and Medicaid Services. The proposed guidance, as subsequently modified by the HHS interim rule issued on August 24, 2009 (described below) establishes the following two methods for securing PHI and PHRs in a manner that would avoid application of the HITECH Act’s breach notification provisions:

- *Encryption*

PHI and PHRs will be deemed unusable, unreadable or indecipherable if the information has been encrypted.²⁸ Encryption for this purpose must comply with the HIPAA Security Rule’s provisions, which define encryption as “the use of an algorithmic process to transform data into a form in which there is a low

²⁵ *Id.* § 13402(h)(1).

²⁶ ARRA § 13402(j).

²⁷ Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg. 19006 (Apr. 27, 2009) (to be codified at 45 C.F.R. pts. 160, 164) [hereinafter Technology Guidance].

²⁸ *Id.* at 19009.

probability of assigning meaning without use of a confidential process or key.”²⁹ For data “at rest” encryption procedures must be consistent with National Institute of Standards and Technology (“NIST”) Special Publication 800-111; and Data in transit will be encrypted for purposes of the proposed rule if encryption complies with Federal Information Processing Standards 140-2. The August interim rule clarified that encryption keys must be kept on a separate device from the data being encrypted. Lastly, access controls, by themselves, do not qualify as encryption so as to render PHI unusable, unreadable or indecipherable to unauthorized individuals. PHI that may be accessed only by individuals with an authorized password is not “secure” for this purpose.

- *Destruction*

PHI and PHRs will be deemed unusable, unreadable or indecipherable if media on which they are stored have been destroyed by one of the following methods: (i) paper, film or other hard copy media have been shredded or destroyed such that PHI and PHRs cannot be read or reconstructed; and (ii) electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88 such that PHI and PHRs cannot be retrieved.³⁰ The August interim rule also clarified that redaction in lieu of destruction is not an acceptable method for securing paper-based PHI.

These approaches, if adopted, “create the functional equivalent of a safe harbor”³¹ with respect to the breach notification provisions contained in the HITECH Act.

(b) *The August 24, 2009 Breach-Notice Guidance*

HHS issued an interim final rule on August 24, 2009,³² establishing standards for notification of breaches of unsecured PHI under the privacy and security rules. The rule clarifies certain key definitions and concepts, generally in a manner that is favorable to covered entities and business associates, while remaining true to the Act and the intent of Congress. The interim final rule also makes minor modifications to, and formally adopts, its April 17, 2009 proposal relating to which technologies and methodologies will render PHI unusable, unreadable, or indecipherable to unauthorized individuals (and, as a consequence, exempt from the Act’s breach notice requirements). HHS has also clarified that the requirements of the HITECH Act are in addition to those of the security rule. Thus, while the security rule does not require encryption in all instances, encryption is necessary to avoid the HITECH breach notice rules.

The bulk of the interim final rule implements the breach notification provisions of the Act as they apply to HIPAA covered entities and their business associates.

²⁹ 45 C.F.R. § 164.304.

³⁰ Technology Guidance, 74 Fed. Reg. at 19010.

³¹ *Id.* at 19008.

³² 74 Fed. Reg. 42740 (Aug. 24, 2009) (This rule will be codified in Part D of Title 45 of the Code of Federal Regulations.)

(i) Breach

Breach is defined to mean “the acquisition, access, use, or disclosure of protected health information...which compromises the security or privacy of the protected health information.” The interim final rule makes clear that the definition of “breach” is limited to PHI. In determining whether notification is required under the Act, therefore, one must first determine whether a use or disclosure violates the privacy rule. This means, among other things, that the breach notice rules do not apply to employment records, which are not PHI. (Notification requirements under other laws may still apply to employment records.) Similarly, breach notice rules do not apply to de-identified health information, again, because it is not PHI and because its disclosure does not violate the privacy rule.

A “breach” must relate to a use or disclosure that “compromises the security or privacy” of PHI. Once it is established that a use or disclosure violates the privacy rule, the covered entity must determine whether the violation compromises the security or privacy of the PHI. Here, HHS determined that the breach must “[pose] a significant risk of financial, reputational, or other harm to the individual” to trigger the obligation to provide notice. This will require covered entities and business associates to perform a risk assessment and use their discretion to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. Covered entities and business associates are also instructed to consider who impermissibly used the information, or to whom the information was impermissibly disclosed, when evaluating the risk of harm to individuals. For example, if PHI is impermissibly disclosed to another covered entity, the chance of significant harm may be more remote, since the recipient is already obligated to protect PHI. Covered entities and business associates should also consider the type and amount of PHI involved in the impermissible use or disclosure. The disclosure of sensitive health information, such as mental health or infectious disease related information, is more likely to create a significant risk of harm.

(ii) Exceptions to Breach

The interim final rule includes the following three exceptions to the definition of “breach”:

1. Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate.

Example: A billing employee receives and opens an e-mail containing PHI about a patient, which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it. Because the billing employee’s use of the information was done in good faith and within the scope of his authority, the disclosure does not constitute a breach.

2. Inadvertent disclosure of PHI from one person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.

Example: A physician in a group practice has authority to use or disclose PHI at a hospital by virtue of participating in an “organized health care arrangement” (e.g., hospital/group health practice). The physician mistakenly provides the wrong patient file to a nurse at the hospital. There is no breach in this instance.

3. Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Example: A covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. The covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable and that the covered entity knows were sent to the wrong individuals, however, should be treated as potential breaches.

(iii) Unauthorized Acquisition, Access, Use, or Disclosure

The interim final rule defines the phrase “unauthorized acquisition, access, use, or disclosure of protected health information” as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted” by the Act. In this regard, HHS helpfully reminds us that, while the HIPAA security rule provides for administrative, physical, and technical safeguards and organizational requirements for electronic PHI, it does not govern uses and disclosures of PHI. Therefore, a violation of the security rule does not itself constitute a potential breach under the Act’s breach notice rules. Such a violation may, however, lead to a use or disclosure of PHI that is not permitted under the privacy rule and, thus, may violate the Act’s breach notice rules.

(iv) Limited Date Sets

The interim final rule contains special rules related to “limited data sets.” A limited data set is created by stripping from PHI 16 direct “identifiers” set out in the privacy rule. These identifiers include the name, address, social security number, and account number of an individual or the individual’s relative, employer, or household member, but not birth dates and zip codes. Because HHS was concerned that birth dates and zip codes increase the potential for re-identification, it was unwilling to provide a blanket exemption from the Act’s breach notice rule for limited data sets. Instead, the interim final rule establishes an exemption for limited data sets where zip codes or dates of birth have been removed. In addition, HHS recognized that there may be instances (based on a risk analysis) that the risk of identifying a particular individual is so small that the use or disclosure of a limited data set poses no significant risk of harm to any

individuals. Note that even if a covered entity is able to avoid breach notice rules through the use of a limited data set, it may still have state law notification obligations.

(v) Notice Requirements

The interim final rule tracks closely the requirements of the Act. Notice of a breach must be provided without unreasonable delay and within 60 days after “discovery.” A breach is “discovered” as of the first day that it is known (or reasonably should have been known) to the covered entity or the business associate. (A business associate that discovers a breach is required to notify the covered entity.) A covered entity or business associate is treated as having knowledge of a breach on the day that any employee, officer, or other agent has such knowledge or should have had such knowledge (except for the individual who committed the breach).

The notice of breach must, at a minimum, contain the following:

- A brief description of the breach, including dates
- A description of types of unsecured PHI involved
- The steps the individual should take to protect against potential harm
- A brief description of steps the covered entity or business associate has taken to investigate the incident, mitigate harm, and protect against further breaches
- Contact information.

The interim final rule requires that the notices be written in plain language and that they not include the actual PHI that was the subject of the breach (e.g., social security numbers). Notices must also tell the individual how to mitigate harm (e.g., by notifying his or her credit card company if the breach included related financial information).

Additional notice requirements include the following:

Written notice must be provided to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual). Notices to minors, incapacitated persons, and deceased persons may be made to their personal representatives.

Where there is insufficient or out-of-date contact information, or in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the Web site of the covered entity or notice in major print or broadcast media is required. Where there is a possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the methods described above. Substitute notice for breaches involving fewer than 10 people may include alternative forms of written notice,

telephone, email, or other means. Where the substitute notice covers more than 10 individuals, a toll-free telephone number must be provided for at least 90 days.

Notice is required to be provided to prominent media outlets within the state or jurisdiction if a breach of unsecured PHI affects, or is reasonably believed to affect, more than 500 residents of that state or jurisdiction.

What constitutes a prominent local media outlet depends on the circumstances. In the case of a small town, an appropriate media outlet may be the local newspaper. In other cases, a prominent local media outlet may be a major general interest newspaper with state-wide circulation. Notices to the media are required, in addition to individual notices.

Notice must be furnished to HHS by covered entities immediately for breaches involving more than 500 individuals and annually for all other breaches.

The guidance contains helpful rules where a breach involves residents in multiple states or jurisdictions. For example, if a covered entity discovers a breach of 600 individuals, 200 of whom reside in Virginia, 200 of whom reside in Maryland, and 200 of whom reside in the District of Columbia, such a breach did not affect more than 500 residents of any one state or jurisdiction. As such, notification is not required to be provided to the media. But if a covered entity discovered a breach of unsecured PHI involving 600 residents within the state of Maryland and 600 residents of the District of Columbia, notification must be provided to a prominent media outlet serving the state of Maryland and to a prominent media outlet serving the District of Columbia.

It is also possible that a breach may occur at a business associate and involve PHI of multiple covered entities. There, a covered entity would only be required to provide notification to the media if the information breached included the PHI of 500 or more individuals located in any one State or jurisdiction. But where the entities are unable to determine which entity's PHI was involved, the covered entities may require the business associate to provide notification to the media on behalf of all of the covered entities.

Generally, covered entities must send the required notification without unreasonable delay, and in no case later than 60 calendar days after the date the breach was "discovered." Covered entities may take reasonable time to investigate the circumstances surrounding the breach, however, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule. Importantly, 60 days is an outer limit. In some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification.

(c) *Regulatory Effective Dates*

The HITECH breach notice rules are generally effective for breaches occurring on or after September 23, 2009. HHS will not impose sanctions for breaches, however, for failure to provide notice of breaches occurring before February 22, 2010. Nevertheless,

the regulators expect Covered Entities and their business associates to use their best efforts to comply during prior to February 22, 2010.

2. Breaches of “Unsecured PHRs”

HITECH for the first time requires vendors of “personal health records” (or PHRs), entities offering products and services through a PHR vendor’s website, to notify affected individuals and the Federal Trade Commission upon discovery of a breach of security of unsecured “PHR health information.”³³ According to a definition provided by the American Health Information Management Associate (AHIMA) in 2005, “PHR” is:

An electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR is separate from and does not replace the legal record of any provider.³⁴

While PHRs can be kept on paper or electronically, the HITECH rules governing PHRs are directed at the latter. Electronic records can be kept via a software application on a personal computer or through an Internet-based service. Google and Microsoft each offer Internet-based PHR services. PHRs are also offered by healthcare providers (e.g., the Department of Veterans Affairs), employers (e.g., Dell and IBM), and insurers (e.g., Blue Cross and Blue Shield Association). Consumers are required to monitor and update information as appropriate. PHR vendors are not covered entities, but they are business associates to the extent that they contract with covered entities.

“Unsecured PHR identifiable health information” is health information contained in a PHR that is not protected through the use of a technology specified by HHS.³⁵ (ARRA § 13407(f)(3) states that the Secretary specifies the technology and methodologies for securing information.) The FTC is required to notify HHS of any breach notices it receives, but it is the FTC and not HHS that has enforcement authority regarding breaches of unsecured PHR health information.

On April 20, 2009, the FTC issued a proposed rule requiring PHR vendors and related entities to provide notice to affected individuals and the FTC when personal health records are acquired without the individual’s authorization.³⁶ Personal health records are broadly defined, and include information that relates to the “payment for the provision of health care”³⁷ (e.g., a database containing names and credit card

³³ *Id.* § 13407(a).

³⁴ AHIMA e-HIM Personal Health Record Work Group, *The Role of the Personal Health Record in the EHR*, Journal of AHIMA 76, no. 7 (July–August 2005): 64A–D.

³⁵ ARRA § 13407(f)(3).

³⁶ Health Breach Notification Rule, 74 Fed. Reg. 17914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

³⁷ *Id.* at 17916.

information), and the mere fact of having an account with a vendor whose products relate to a particular health condition is itself is sufficient to create a PHR. These rules apply to PHR vendors, PHR-Related Entities, and Third-Party Service Providers, which are together referred to “covered entities.” The reference to “covered entities” is particularly confusing in this context since the FTC breach notification rules do *not* apply to HIPAA-covered entities or to an entity’s activity as a business associate of a HIPAA-covered entity, both of which are subject to regulation under HIPAA. These rules are instead directed toward entities such as web-based applications dedicated to assisting consumers manage their medications, or offer online personalized health checklists, or advertise dietary supplements online, etc.

The FTC’s proposed regulation imposes on Vendors of PHR or a PHR-Related Entity that discover a breach of security involving unsecured PHR the requirement to notify the FTC and each affected individual.³⁸ Third-party service providers are required to notify the PHR Vendor or the PHR-Related Entity, which in turn must notify the affected individual and the FTC. The FTC is required to notify HHS of the breach notifications it receives.

For purposes of the FTC’s proposed rule, the following definitions apply:

- *Vendor of PHR* means an entity (other than a HIPAA-covered entity or business associate) that offers or maintains a personal health record. A personal health record is an electronic record of identifiable health information that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.³⁹
- *PHR-Related Entity* means an entity (other than a HIPAA-covered entity or business associate) that offers products or services through the website of a PHR Vendor or through a HIPAA-covered entity, or that accesses information in a PHR or sends information to a PHR.⁴⁰
- *Third-party service provider* means an entity that provides services to a Vendor of PHR or to a PHR-Related entity, and which accesses, maintains, uses, stores, or discloses PHR as a result of its services (e.g. billing or data storage services).⁴¹

A breach is discovered on the first day it is known or should reasonably have been known. Notification of the breach must be given “without unreasonable delay” and in no case later than 60 days after discovery of the breach.⁴² In some cases, it may be unreasonable to wait 60 days. The notice to individuals must describe how the breach occurred (including the date of the breach and date of discovery), the types of unsecured PHR identifiable health information that were involved, the steps individuals should take

³⁸ *Id.* at 17917.

³⁹ *Id.*

⁴⁰ *Id.* at 17916.

⁴¹ *Id.*

⁴² *Id.* at 17918.

to protect themselves from harm, a description of the steps the entity is taking to mitigate the breach, and contact information for the individuals including a toll-free number, e-mail address, website, or postal address.

The breach notice rules are similar to those imposed on HIPAA covered entities. Notice from the Vendor of PHR or the PHR-Related Entity to the affected individuals must be provided in writing by first class mail or, where urgent, by telephone or other means in addition to first class mail.⁴³ Where ten or more individuals are affected and they cannot be reached through those methods, notice must be given either through posting on the Vendor of PHR or PHR-Related Entity's website homepage for a period of six months, or in major print or broadcast media reasonably calculated to reach the affected individuals. Where 500 or more residents of a state are affected by a breach, the Vendor of PHR or PHR-Related Entity must provide notice to prominent media outlets serving the state.

In connection with the promulgation of a final rule, the FTC has solicited comments on (i) the nature of the entities to which the rules should apply, (ii) the particular products and services they offer, (iii) the extent to which Covered Entities may be HIPAA-covered entities or business associates, (iv) whether some vendors of PHR may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of PHR to the public, and (v) circumstances where a dual role may lead to receipt of multiple breach notices.⁴⁴

FTC is directed to issue interim final regulations on or before August 16, 2009, and the rule will take effect 30 days thereafter.⁴⁵

D. *Revisions to the "Minimum Necessary" Standard*

The HIPAA privacy rule includes a "minimum necessary standard" under which a covered entity that uses or discloses PHI or requests such information from another covered entity must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use or disclosure.⁴⁶ Exceptions to the minimum necessary standard include requests by a health care provider for treatment purposes, and the disclosure of a "limited data set" for certain specified purposes generally relating to research. A limited data set has most direct identifiers removed and is considered to pose a low privacy risk.

HITECH directs HHS to issue guidance by August 2010 establishing the contours of what constitutes the minimum necessary standard.⁴⁷ In the meantime, a covered entity may only use, disclose, or request limited data set information. If more information is needed, the covered entity may comply with the current minimum necessary standard. In developing guidance on what constitutes "minimum necessary," HHS is required to take

⁴³ *Id.* at 17924.

⁴⁴ *Id.* at 17915.

⁴⁵ ARRA § 13407(g)(1).

⁴⁶ 45 C.F.R. § 164.502(b).

⁴⁷ ARRA § 13405(b).

into consideration the information necessary to improve patient outcomes and to manage chronic disease. For the purpose of developing regulations on the accounting of disclosures, HHS must take into account an individual's interest in learning when the PHI was disclosed and to whom, as well as the cost of accounting for such disclosures.⁴⁸ HHS must also review and evaluate the definition and, to the extent necessary, eliminate those activities that could reasonably and efficiently be conducted using de-identified information or those that should require authorization. HHS is also directed to evaluate the impact of charging an amount to cover the costs of preparing and transmitting data for public health or research activities.

The HITECH modifications to the minimum necessary standard take effect August 17, 2010.⁴⁹

E. *Restrictions on Sales of PHI*

HITECH generally bars covered entities and business associates from receiving remuneration, directly or indirectly, for any PHI without patient authorization specifically addressing sale.⁵⁰ This prohibition is subject to exceptions for public health activities, research, certain expenses relating to treatment, payment and health care operations, to provide an individual with his/her PHI, and in other instances permitted by regulation.

HHS is directed to issue regulations no later than August 2010, and the restrictions on the sale of PHI will take effect six months thereafter.⁵¹

F. *Patient Access to and Restrictions on PHI*

The HIPAA privacy rule generally provided individuals with the right to see and obtain a copy of their PHI.⁵² The covered entity can impose reasonable fees for providing the information. Individuals also have the right to amend or supplement their own PHI and the right to request that a covered entity restrict the use and disclosure of their PHI for the purposes of treatment, payment, or health care operations. However, the covered entity is not required to agree to such a restriction unless it has entered into an agreement to restrict it. Finally, individuals have the right to an accounting of disclosures of their PHI by a covered entity during the previous six years, with certain exceptions.

HITECH expands individual rights by giving individuals the right to receive an electronic copy of their PHI if it is maintained in an electronic health record.⁵³ Any associated fee charged by the covered entity can only cover its labor costs for providing the electronic copy. Covered entities must also honor a patient's request that the PHI regarding a specific health care item or service not be disclosed to a health plan for purposes of payment or health care operations, if the patient paid out-of-pocket in full for

⁴⁸ *Id.* § 13405(c).

⁴⁹ *Id.* § 13405(b)(1)(B).

⁵⁰ *Id.* § 13405(d).

⁵¹ *Id.* §§ 13405(d)(3)-(4).

⁵² 45 C.F.R. § 164.502(a).

⁵³ ARRA § 13405(e).

that item or service.⁵⁴ Individuals must also be given an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment, and health care operations during the previous three years, if the disclosures were through an electronic health record.⁵⁵

HHS is directed to issue regulation implementing the new patient access rules by September 15, 2009. The rule will take effect 30 days thereafter.

G. *Marketing*

Before HITECH, the HIPAA privacy rule generally permitted covered entities to use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual's authorization and with few restrictions.⁵⁶ The term "health care operations" was broadly defined to include quality assessment and improvement activities, case management and care coordination, evaluation of health care professionals, underwriting, legal services, business planning, customer services, grievance resolution, and fundraising.⁵⁷ But a covered entity was not allowed to disclose health information to a third party (e.g., a pharmaceutical company) in exchange for direct or indirect remuneration, or for the marketing activities of the third party without first obtaining a patient's authorization.⁵⁸ Similarly, a covered entity could not use or disclose health information for its own marketing activities without authorization.

"Marketing" for this purpose is defined as a communication *about* a product or service that encourages the recipient to purchase or use the product or service.⁵⁹ Importantly, communications made by a covered entity (or its business associate) to encourage a patient to purchase or use a health care-related product or service are excluded from this definition and, therefore, do not require the patient's authorization, even if the covered entity was paid by a third party to engage in such activities.

Under HITECH, *any* communication by a covered entity or a business associate about a product or service or one that encourages the recipient to purchase or use a product or service is not considered to fit within the "health care operations exception" unless the communication (i) describes a health-related product or service or payment for a health-related product/service, (ii) is related to treatment, or (iii) is used for case management or care coordination for the individual or to direct or recommend certain alternative treatments, therapies, health care providers, or settings of care to the individual.⁶⁰ Fundraising activities using a patient's protected health information are still permitted, so long as any written fundraising provide an opportunity to opt out of future fundraising communications.

⁵⁴ *Id.* § 13405(a).

⁵⁵ *Id.* § 13405(c).

⁵⁶ 45 C.F.R. § 164.502(a).

⁵⁷ *Id.* § 164.501.

⁵⁸ *Id.* § 164.503(a)(3).

⁵⁹ *Id.* § 164.501.

⁶⁰ ARRA § 13406(a)(1).

H. *Enforcement*

HIPAA includes criminal penalties that apply in the case of violations of the privacy rules.⁶¹ Penalties include fines of up to \$250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm. But, only covered entities can be prosecuted under these rules.

Similarly, HIPAA authorized the Secretary of HHS to impose civil monetary penalties on any person failing to comply with the privacy and security standards.⁶² The maximum civil fine is \$100 per violation and up to \$25,000 for all violations of an identical requirement or prohibition during a calendar year.⁶³ Civil monetary penalties may not be imposed if (i) the violation is a criminal offense, (ii) the person did not have actual or constructive knowledge of the violation, (iii) the failure to comply was due to reasonable cause and not to willful neglect, and was corrected promptly (within 30-days).⁶⁴

HITECH expands the HIPAA criminal penalties for wrongful disclosure of PHI to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether or not they are employees of the covered entity.⁶⁵ HITECH also amends HIPAA to permit the HHS Office for Civil Rights (or “OCR”) (the agency previously charged with enforcing the HIPAA civil penalty provisions) to pursue an investigation and to impose civil monetary penalties against any individual for an alleged criminal violation of the privacy or security rules if the Justice Department declines to prosecute. HHS is directed to conduct periodic audits of covered entities and business associates in an effort to ferret out both willful violations and “willful neglect” of the rules.⁶⁶ HHS is also directed to issue regulations implementing these changes. Penalties collected will be applied to enforcing the HIPAA privacy and security standards.⁶⁷

State Attorneys General are also allowed to bring a civil action in Federal district court against individuals who violate the HIPAA privacy and security standards, and they can seek damages of up to \$100 per violation, capped at \$25,000 for all violations of an identical requirement or prohibition in any calendar year.⁶⁸ State action against a person would not be permitted, however, if there is a federal civil action pending against the same individual. HITECH also adds a mechanism for individuals to recover a portion of HHS civil penalty or monetary settlements.

⁶¹ 42 U.S.C. § 1320d-6.

⁶² *Id.* § 1320d-5.

⁶³ 45 C.F.R. § 160.404.

⁶⁴ *Id.* § 160.410.

⁶⁵ ARRA § 13409.

⁶⁶ *Id.* § 13411.

⁶⁷ *Id.* § 13410(c)(1).

⁶⁸ *Id.* § 13410(e).

Lastly, HITECH increased the penalties for violations of the HIPAA privacy and security rules as follows:⁶⁹

- Tier 1. If a person is not aware of the violation (and would not have known with reasonable diligence), the penalty is at least \$100/violation, not to exceed \$25,000 for all violations of the same requirement in the same calendar year.
- Tier 2. If a violation is due to “reasonable cause” (but not willful neglect), the penalty is at least \$1,000/violation, not to exceed \$100,000 for all violations of the same requirement in the same calendar year.
- Tier 3: If a violation is due to willful neglect and is corrected in 30 days, the penalty is at least \$10,000/violation, not to exceed \$250,000 for all violations of the same requirement in the same calendar year.
- Tier 4. If a violation is due to willful neglect and is not corrected in 30 days, the penalty is at least \$50,000/violation, not to exceed \$1.5 million for all violations of the same requirement in the same calendar year.

The HITECH rules governing civil and criminal penalties take effect two years following the date of ARRA’s enactment, or February 17, 2011.⁷⁰ The provisions allowing individuals to recover a portion of HHS civil penalty or monetary settlements take effect three years following the date of ARRA’s enactment, or February 17, 2012.⁷¹

III. Conclusion

ARRA has both raised and broadened the HIPAA compliance bar. Business associates, which previously had been given something of a free pass, are now subject to the old and new rules, including the newly expanded enforcement provision. The effective dates for these various provisions cascade out over the next three years, with most of the substantive requirements taking effect within the first 18 months following enactment. Though some guidance has already been issued in the form of proposed rules, much more work needs to be done on the part of the agencies.

The changes wrought by HITECH will pose challenges to covered entities, business associates and PHR vendors, among others. Business associate agreements will need to be reviewed and updated to comply with HITECH’s new rules, and employees with access to PHI will need to be trained. Covered entities and business associates should begin now to understand these new rules and to prepare for their ultimate implementation. In particular, this will require covered entities to revisit their business associate agreements and to train their employees. They will also need to amend “audit” practices so as to be in a position to comply with the expanded disclosure requirements.

⁶⁹ *Id.* § 13410(d).

⁷⁰ *Id.* § 13410(b)(1).

⁷¹ *Id.* § 13410(c)(3).