



NACHC Issue Brief
Changes to the Health Insurance Portability and Accountability Act
Included in ARRA

March 2010

Prepared By:
Marisa Guevara
and
Marcie H. Zakheim

Feldesman Tucker Leifer Fidell, LLP
2001 L Street, NW Second Floor
Washington, DC 20036
202.466.8960



This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is published with the understanding that the publisher is not engaged in rendering legal, financial, or other professional service. If legal advice or other expert advice is required, the services of a competent professional should be sought.

This publication was supported by Grant/Cooperative Agreement Number U30CS16089 from the Health Resources Services Administration, Bureau of Primary Health Care (HRSA/BPHC). The contents of this publication are solely the responsibility of the author(s) and do not necessarily represent the official views of HRSA/BPHC.

Changes to the Health Insurance Portability and Accountability Act Included in ARRA

While most people have focused solely on the millions of dollars in funding available through the American Recovery and Reinvestment Act (ARRA), a key piece of innovation and investment promoted by the legislation is in the area of health information and technology. Title XIII of ARRA, also known as the Health Information Technology for Economic and Clinical Health or the HITECH Act, addresses both new grant programs and initiatives by the Federal government to encourage the use of health information technology as well as changes to the existing Privacy and Security Regulations that are a part of the Health Insurance Portability and Accountability Act (HIPAA). These HIPAA-related changes are the focus of this Issue Brief.

The changes made by the HITECH Act amend the following pieces of HIPAA:

- Enforcement Provisions
- Business Associates
- Accounting of Disclosures
- Request for Records
- Minimum Necessary Standard

The HITECH Act also adds a new section to HIPAA – the Breach Notification Rule.

The majority of these changes will become effective in **February of 2010**, a year after the President signed ARRA. Others, like the Breach Notification Rule, become effective sooner. Specifically, the Breach Notification Rule applies to breaches discovered on **or after October 23, 2009**, although the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR), which has the responsibility for enforcing the Privacy Rule and the Security Rule, has determined **that it will not seek enforcement of the new Breach Rule until February 2010**.

This Issue Brief addresses the changes listed above. Each section begins with a list of the most important facts to know about that change, followed by detailed explanations regarding the changes, and where possible, suggestions for compliance.

BREACH NOTIFICATION RULE

Perhaps the most extensive changes occurred in the area of breach notification. Section 13402 of the HITECH Act (as interpreted by HHS through an Interim Final Rule published in the Federal Register on August 23, 2009) provides the basic requirements for notification in case of a breach of unsecured Protected Health Information (PHI). The following are a few important facts concerning the Breach Notification Rule (the Rule):

- **To what does the Rule apply?** The Rule applies to breaches discovered thirty days after September 23, 2009.
- **When does this Rule take effect?** While the Rule applies to breaches discovered on or after October 23, 2009, HHS has announced that it will not seek enforcement of these provisions until February 17, 2010, when the other provisions of the HITECH Act take effect.
- **Who is subject to this Rule?** Covered entities and their business associates that access, store or transmit “unsecured PHI” must comply with the Rule. The definition of “unsecured PHI” will be discussed below.
- **What do I have to do under this Rule?** If you are subject to this Rule, you must provide **written** notice to individuals whose information may have been accessed that you have discovered a breach. This notice has several components that will be discussed below. You must also keep a log of all discovered breaches.

What is a breach?

The Rule defines a breach as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy and Security Rules] which compromises the security and privacy of the protected health information.”¹ The definition also states that to “compromise the security and privacy of the [PHI]” means to “poses a significant risk of financial, reputational, or other harm to the individual.”² In addition, a use or disclosure of PHI that is considered a limited data set (as defined under 45 C.F.R. § 164.512(e)(2)) and that does not contain either date of birth or zip code does not compromise the security and privacy of the PHI.³ Finally, the definition includes three situations that are excluded from the definition of breach, meaning that these occurrences will not trigger the breach notification process because they are not considered breaches:

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use:
 - Was made in good faith; and
 - Was made within the scope of authority; and
 - Does not result in further use or disclosure in a manner not permitted under subpart E of this part.

Example – If an employee accidentally accesses PHI that he or she has authority to access and there is no further disclosure. If a nurse is searching for the electronic record

¹ 45 C.F.R. § 164.402

² *Id.*

³ *Id.*

for a patient “Doe, James” but instead accesses the record for “Doe, Jamie” this would not be a breach because it is protected by the first exception.

- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

Example – In the example above, if the nurse emailed the PHI of “Doe, Jamie” to another nurse at the covered entity, this would be protected under the second exception.

- A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Example – This last exception is a little more confusing. The example given by HHS in the preamble of the regulation is a situation in which a covered entity mails Explanations of Benefits (EOBs) to the wrong individuals, but those EOBs are returned to sender unopened. While this situation does not seem likely, in the event that something of this nature occurs, it is not considered a breach.

A final point to remember is that to meet the definition of breach, the use or disclosure must be a violation of the Privacy Rule, *i.e.*, the use or disclosure is not one that is currently authorized under law (such as disclosure for treatment purposes).⁴

What is unsecured PHI?

There cannot be a breach unless unsecured PHI is involved. The Rule defines “unsecured protected health information” as “protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology *specified by the Secretary in guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS web site.*” (Emphasis added). The guidance issued by the Secretary to which that phrase refers was published on April 27, 2009 (74 *Fed. Reg.* 19006) and specifies encryption and destruction as the technologies and methodologies for securing PHI.

Encryption, for the purposes of the breach notification rule and the guidance issued by the Secretary, means “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and no one has improperly acquired the key.⁵ To prevent unauthorized access to the key, the guidance recommends storing decryption tools on a device or location separate from the data

⁴ 74 *Fed. Reg.* 42744 (August 23, 2009)

⁵ 74 *Fed. Reg.* 42742. This is the same definition of encryption found in the Security Rule at 45 C.F.R. § 164.304.

that is being encrypted or decrypted.⁶ For specific methodologies of encryption that meet the standards, users are referred guidelines for data at rest and data in motion published by National Institute for Standards and Technology (NIST), an agency within the Department of Commerce.

In terms of destruction, the guidance requires hard copy media to be “shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed” and does not include redaction.⁷ Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.⁸

The key point is this – if the PHI is encrypted or destroyed, it is secured and, thus, the breach notification provisions do not apply. From this perspective, the Rule acts as a deterrent measure – it seeks to encourage covered entities, like health centers, to store and transmit PHI in a secured format, so that it will avoid the burdens of breach notification. The other significant deterrent provision is a requirement discussed in greater detail below – specifically, if a breach impacting a certain number of people occurs, the covered entity is required to notify local media outlets.

How to Determine a Breach Has Occurred:

1. Is there an impermissible use or disclosure of PHI that violates the Privacy Rule?
 - a. If the answer is yes, go to question 2.
2. Did or does the impermissible use or disclosure pose a significant risk of financial, reputational, or other harm to the individual?
 - a. If the answer is yes, go to question 3.
3. Does the incident fall under one of the exceptions discussed above?
 - a. If the answer is yes, then there is no breach.
 - b. If the answer is no, then there is a breach.

It is important to document all steps of this analysis. Under 45 C.F.R. § 164.414, the covered entity must prove that no breach occurred or, in the case of a breach, that all required notifications were sent. To protect itself, each health center should keep records of all notices sent regarding a breach as well as all information gathered in the process of determining whether a breach occurred. In many cases it may be beneficial to the health center to designate an individual within the organization, likely the Privacy Officer, as the contact person for the Breach Notification Rule and as the custodian of records related to the Rule.

⁶ *Id.*

⁷ 74 *Fed. Reg.* 42743

⁸ *Id.*

What's in a Notice?

Notice to individuals whose PHI has been or is reasonably believed to have been breached must include the following five elements:

- A brief description of what happened, including the date of the breach and the date that the breach was discovered. The discovery date would be the date that the breach was or should have been discovered.
- A description of the types of unsecured PHI that were involved. **IMPORTANT:** do not include the actual information, as that, in and of itself, would violate the Privacy Rule.
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the covered entity and/or business associate involved is doing to investigate the breach, to mitigate the harm to individuals, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site, or postal address.

The notice must be written in plain language and be easily understood by patients and other individuals. Of note, in providing notice, health centers may be subject to other rules governing communications with patients (*e.g.*, the Civil Rights Act of 1964, the Americans with Disabilities Act) and/or to other guidance on appropriate communications with patients whose primary language is not English (*e.g.*, guidance from the Office of Civil Rights on providing services to Limited English Proficiency patients). Thus, health centers may be required to provide notice in multiple languages or multiple formats so that all patients receive meaningful notice in a manner that allows them to understand the notice. Health centers should be mindful of these obligations as notice must comply with all applicable laws, not just the Rule.

To Whom Must Notice Be Sent?

As noted above, notice must be sent to any individual whose information was, or was reasonably believed to have been, accessed, acquired, used or disclosed during the breach. If the breach affects more than five hundred (500) individuals residing in the same state, notice must also be sent to prominent media outlets in that area, as well as to HHS so that it can be posted on the web site.

Notice to Individuals

Notice to individuals must be written and mailed to the last known address of the individual via first class mail. However, if the individual has agreed to receive notices and other communications from the health center via electronic mail, notice may be sent by e-mail. If the individual is a minor or otherwise lacks legal capacity, providing notice to the parent or personal representative will satisfy the requirement to provide notice to the individual. (In providing notice to a personal representative, be mindful of the existing HIPAA laws and state laws on minors and personal representatives). In the case of a deceased individual whose information has been breached, notice should be sent to the last known address of the next of kin.

If the covered entity does not have current or complete address or contact information for an individual affected by the breach, substitute notice must be provided. The format of substitute notice will depend on how many individuals require substitute notice:

- If substitute notice is necessary for less than ten (10) individuals, it may be provided by telephone, email or other alternate means. In this situation you may provide notice by email even if the individual has not previously agreed to receive notice by email. In providing substitute notice, be careful:
 - Not to disclose more information than necessary; and
 - Not to unnecessarily disclose PHI.

If you are leaving a message, leave a name and number for the individual to return the call, rather than the specifics regarding the breach.

- If substitute notice is necessary for more than ten (10) individuals, then notice must be provided either:
 - On the home page of the health center's web site – notice provided on a website must be posted for ninety (90) days and must be conspicuous, and the content of the notice may be accessible through a hyperlink; or
 - In major print or broadcast media in geographic areas where individuals affected by the breach likely reside (*i.e.*, the health center's service area) – notice in print media must also be conspicuous.

Regardless of whether the health center uses its website or print/broadcast media as the means of substitute notice, the health center must also provide a toll-free number for individuals to call to learn if their information was affected.

The burdensome requirements of providing substitute notice where more than 10 individuals are affected demonstrates the deterrent nature of this requirement. Rather than being prepared to post notice on the website, the newspaper or the news, it is much more efficient

and effective to institute a practice under which the health center regularly updates contact information for its patients.

Notice to the Media

If the breach involves the information of five hundred (500) or more individuals living in the same State, city, county, or town, the covered entity must notify prominent media outlets located in that jurisdiction. This notice supplements the notice provided to individuals (as discussed above) and should contain the same information and be provided in the same timeframe as the individual notice.⁹ Notice to media outlets may be provided in the form of a press release.¹⁰ In some situations this could be as easy as sending a short press release to a local television station or newspaper. However, not all situations will be that simple. For example, if the breach affects individuals across a State, and there is no single media outlet covering the entire State, then notice will have to be provided to multiple media outlets across the State to ensure compliance with this requirement.

Notice to HHS

Notice of breaches of unsecured PHI must be provided to HHS, but the scope of the breach will determine when that notice must be provided. If the breach involves the information of five hundred (500) or more individuals, HHS must be notified at the same time as notification to the individuals affected – without unreasonable delay and within 60 days of discovery of the breach. If the breach affects less than 500 individuals, the breach should be recorded in a log that will be submitted to HHS annually within 60 days of the end of the calendar year. Under federal law, the log must be maintained for a period of six (6) years; however, State record retention laws may require that the log be kept longer.

In accordance with the dictates of the HITECH Act and the regulations, HHS has posted on its website instructions on submitting notice to the agency. That guidance can be accessed at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>. HHS created an online form to be used for submission purposes. The form requires covered entities to classify the type of breach from a drop-down menu with the following options:

- Theft
- Loss
- Improper Disposal
- Unauthorized Access
- Hacking/IT Incident
- Other
- Unknown

⁹ 74 *Fed. Reg.* 42752 (August 24, 2009)

¹⁰ *Id.*

A breach may fall into multiple categories and the submitter may select multiple categories. Unfortunately, the form does not appear to have supplemental instructions on how to classify the breach you are reporting. Hopefully HHS will issue some guidance or an instruction sheet on completing the form. When filling out the form, it may be helpful to consult an IT specialist to provide guidance on the type of breach, the location of the breach, the safeguards that were in place at the time of the breach and the actions taken in responding to the breach.

Although federal law requires maintenance of a log to record breaches affecting less than 500 individuals (similar to the log of disclosures of PHI maintained by covered entities under the Privacy Rule), the guidance on the HHS website requires covered entities to submit the electronic form described above for each breach. According to the HHS guidance, the only difference in reporting breaches is in the timing – breaches affecting less than 500 individuals may be reported at any time before 60 days after the end of the calendar year, while breaches affecting more than 500 individuals must be reported within 60 days of the date of discovery of the breach.

Before clicking the submit button on the form, the health center should print a copy of the form for its records. HHS will post a list of breaches that affect more than 500 individuals, but, as of the date this Issue Brief was drafted, there were no breaches listed; thus, it is not possible at this time to determine what information about the breach HHS will post.

What if the Breach is of Unsecured PHI in the Control of a Business Associate?

A business associate that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured PHI must notify the covered entity when it discovers a breach of such information.¹¹ If a business associate maintains unsecured PHI for multiple covered entities, it must only notify the covered entity whose information was breached. If, however, the business associate cannot make that determination, it must notify all covered entities that it has experienced a breach of unsecured PHI.¹²

A breach is treated as discovered by a business associate on the first day that such breach is known or should have been known to an employee, officer, or agent of the business associate.¹³ The notification process is as follows:

- Notice to the covered entity must be provided by the business associate without unreasonable delay and not later than 60 days after the date of discovery.
- Once notified, a covered entity has up to 60 days, but without unreasonable delay, to provide notice to individuals, with one exception – if the business associate is an agent

¹¹ 74 *Fed.Reg.* 42753 (August 24, 2009); *see also* 45 C.F.R. § 164.410(a)(1)

¹² *Id.*

¹³ 45 C.F.R. § 164.510(a)(2)

of the covered entity, the covered entity has only 60 days from the date of discovery by the business associate because the knowledge of the business associate is imputed to the covered entity.¹⁴

Notice to the covered entity by the business associate must include, to the extent possible, the identity of each individual whose information has been, or is reasonably believed to have been, breached.¹⁵ In addition, business associates must provide the covered entity with any other information that the covered entity must provide in the notice to individuals (*e.g.*, date of discovery and measures taken to mitigate the harm of the breach).

The preamble to the Rule also provides that “business associates and covered entities will continue to have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals”¹⁶ While the covered entity has the ability to require the business associate to provide notice and should reserve that right in contracts with the business associate, the decision of who will provide notice should be made on a case by case basis.

Law Enforcement Delay

Similar to HIPAA’s Privacy Rule, the Rule recognizes that the needs of law enforcement will sometimes be at odds with the Rule’s requirements and carves-out special, limited exceptions for dealing with law enforcement in such situations. The Privacy Rule addresses circumstances under which a covered entity is allowed to disclose PHI to law enforcement without first obtaining authorization from the individual. In the case of the Breach Notification Rule, the law enforcement exception requires covered entities and business associates to delay notification to individuals for a certain, limited time upon written notice from the law enforcement official that notification “would impede a criminal investigation or cause damage to national security.”¹⁷ A law enforcement official may request a delay in notification orally, but the covered entity or business associate

- Must document the request, including the name of the official making the request; and
- Can only delay for up to thirty (30) days, unless the oral request is supplemented with a written request that specifies the time period for delay.¹⁸

Other Administrative Requirements Related to the Breach Notification Rule

There are several administrative requirements of the HIPAA Privacy and Security Rules that also apply to the Breach Notification Rule. These provisions require the covered entity to:

¹⁴ Federal common law controls the determination of whether a business associate is an agent of the covered entity. In most instances the business associate will be a contractor of the covered entity, not an agent.

¹⁵ 45 C.F.R. § 164.410(c)

¹⁶ 74 *Fed. Reg.* 42754 (August 24, 2009)

¹⁷ 45 C.F.R. § 164.412

¹⁸ 45 C.F.R. § 164.412(b)

- Train members of its workforce on the policies and procedures with respect to PHI and the Breach Notification Rule.¹⁹
- Provide a process for individuals to make complaints regarding the covered entity's policies and procedures relating to PHI and the Breach Notification Rule.²⁰
- Establish a procedure that provides and applies appropriate sanctions to members of its workforce that fail to adhere to the covered entity's policies and procedures relating to PHI and the Breach Notification Rule.²¹
- Not take any retaliatory action against any individual exercising his/her rights under the Privacy Rule, Security Rule, or the Breach Notification Rule.²²
- Implement policies and procedures with respect to PHI that are designed to comply with the Privacy Rule, the Security Rule, and the Breach Notification Rule.²³

ENFORCEMENT PROVISIONS

Civil Monetary Penalties

The HITECH Act expands the enforcement provisions in HIPAA with the goal of strengthening enforcement for violations of the HIPAA Privacy and Security Rules. To do this, Congress:

- Created categories of violations with corresponding tiers of civil monetary penalties (CMPs), the more severe the violation, the higher the penalty; and
- Eased the restrictions on HHS to impose civil monetary penalties for violations.

The changes in the HITECH Act can be found in Section 13410(d) of that Act and are amendments to 42 U.S.C. § 1320d-5.

Unlike the Breach Notification Rule, the changes to the CMPs were effective upon passage of the HITECH Act, or **on February 18, 2009**. HHS, the agency in charge of enforcement of CMPs, released an Interim Final Rule on the enforcement provisions on October 30, 2009. These regulations **became effective on November 30, 2009**.

Under the old enforcement system of CMPs, HHS could impose a fine of up to \$100 for each violation of the HIPAA rules, but could not exceed \$25,000 in a single calendar year for a single covered entity. Further, HHS could not impose a penalty in the following circumstances:

¹⁹ 45 C.F.R. § 164.530(b)(1)

²⁰ 45 C.F.R. § 164.530(d)(1)

²¹ 45 C.F.R. § 164.530(e)(1)

²² 45 C.F.R. § 164.530(g)(1)

²³ 45 C.F.R. § 164.530(i)(1)

- For violations subject to the criminal enforcement provisions;
- Where the person did not know and could not have known through reasonable diligence that they violated the provisions; and/or
- If a failure to comply with the provisions was due to reasonable cause and not willful neglect, and the error was corrected within 30 days.²⁴

These restrictions on HHS’ authority to impose CMPs remain in place.²⁵

The new system of tiered penalties for different violations can best be explained with a chart:

Type of Violation	Amount of Civil Monetary Penalty
The person did not know (and by exercising reasonable diligence would not have known) that he/she violated such provision	\$100 to \$50,000 for each violation
The violation was due to reasonable cause and not willful neglect	\$1,000 to \$50,000 for each violation
The violation was due to willful neglect but was corrected within 30 days	\$10,000 to \$50,000 for each violation
The violation was due to willful neglect but was not corrected within 30 days	\$50,000 for each violation

The maximum amount of penalties that can be imposed on a covered entity in a single calendar year is capped at \$1,500,000. In determining the specific amount of a penalty within the appropriate range, HHS will consider the nature and extent of the violation, the nature and extent of the resulting harm, and other factors set forth at 45 C.F.R. § 160.408, including whether the imposition of the penalty would jeopardize the entity’s ability to provide health care services, the size of the covered entity, and any other factors that justice requires.²⁶ These last factors provide good arguments for health centers to receive reduced penalty fees, but it may take some negotiation with HHS.

BUSINESS ASSOCIATES

Before the HITECH Act, business associates (BAs) were not directly liable for violations of HIPAA. Rather, the covered entity had to obtain assurances from the BA that it complied with the Privacy and Security Rules. **Changes through the HITECH Act now allow HHS to enforce HIPAA directly against BAs.** This could have a significant impact on the relationship between a covered entity and its BAs.

²⁴ 74 *Fed.Reg.* 56124 (October 30, 2009)

²⁵ 45 C.F.R. § 164.410(b)

²⁶ 74 *Fed.Reg.* 56128 (October 30, 2009)

- First, BAs will be directly responsible for compliance with the Administrative Safeguards, Physical Safeguards, Technical Safeguards and Policies and Procedures and Documentation Requirements of the HIPAA Security Rule.²⁷
- Second, BAs will be subject to the civil and criminal penalties under HIPAA for violations of any of the requirements listed above.
- Third, if BAs have knowledge of a pattern of noncompliance with the Privacy Rule by the covered entity, the BA has an obligation to terminate the agreement between itself and the covered entity.
- Lastly, BA agreements will be required for health information exchanges, regional health information organizations, e-prescribing gateways, and other similar arrangements, as well as with vendors contracted with a covered entity to provide a Personal Health Record (PHR) as part of an Electronic Health Record (EHR).²⁸

HHS has not yet issued regulations regarding these additional obligations of BAs, so there is little guidance in terms of how the new provisions will be implemented. **However, health centers should consider amending their BA agreements now in order to alert BAs of their new obligations and liabilities.** It is important to keep in mind that, although the BA is directly responsible for compliance and may have penalties imposed directly for HIPAA-related violations, the health center’s obligations with respect to the conduct of its BAs has not been obviated (*i.e.*, health centers must continue to ensure the compliance of its BAs). Rather, these changes could have a large impact on the obligations of the BA, particularly in terms of compliance with the Technical Safeguards of the Security Rule.

CHANGES IN AN INDIVIDUAL’S RIGHTS RELATED TO THEIR PHI

The HITECH Act provides expansions or adaptations to an individual’s rights related to their PHI. The Privacy Rule gives individuals the right to:

- Request and receive an accounting of the disclosures of their PHI, with certain limited constraints.
- Receive a copy of his/her entire medical record.

²⁷ 45 C.F.R. § 164.308, 164.310, 164.312, and 164.316, respectively

²⁸ The HITECH Act defines a PHR as 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. An EHR is defined as “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.”

The HITECH Act expands these obligations for covered entities using an EHR system and also includes one change applicable to all covered entities (regardless if whether they use an EHR system or paper records). These changes are discussed in greater detail below.

Accountings of Disclosures

Prior to the HITECH Act, when providing a patient with an accounting of disclosures, covered entities were not required to include disclosures made for treatment, payment or healthcare operations. The HITECH Act now requires only those covered entities using EHR systems to provide a full accounting of disclosures of a patient's PHI, including disclosures that were made for treatment, payment, or health care operations. At the same time the amount of information to be provided is increased, and the length of time for which the accounting covers is shortened from six years to three years. **(Please note that these changes do not apply to covered entities that do not use an EHR system).**

While these changes do not take effect immediately, their impact is staggered depending on when the entity began (or begins) to use an EHR system.

- If the covered entity was using an EHR system as of January 1, 2009, the new requirements will apply to disclosures made on or after January 1, 2014.
- If the covered entity adopts an EHR system after January 1, 2009, the new requirements will apply to disclosures made on or after January 1, 2011 or the date when the covered entity begins using the EHR system, whichever is later.

In this respect, Congress has rewarded those covered entities that already adopted EHR systems because they are not subject to the more cumbersome requirements. At the same time, Congress has built in necessary time to allow the programmers and developers of EHRs to write programs that will track all the necessary information.

In addition to the changes applicable solely to covered entities using EHR systems, all covered entities that have been presented with a request for an accounting of disclosures may:

- Provide to the individual disclosures of that individual's PHI by the covered entity and its BAs; or
- Provide to the individual disclosures of the individual's PHI by the covered entity and a list of the entity's BAs from which the individual make seek separate accountings of disclosures.

Health centers should protect their right to pass along the obligation to provide, upon request, an accounting of disclosures made by their BAs by inserting in their BA agreements an addendum that puts the BA on notice that it may be required to respond directly to an

individual's request for an accounting of disclosures, and that the BA therefore must have systems in place to comply with the legal requirements for providing accountings of disclosures.

An Individual's Right to Request a Copy of His or Her Record

As noted above, the Privacy Rule provides an individual the right to request a copy of his or her medical record and allows the covered entity to charge the individual a reasonable, cost-based fee for copying and postage and the time it takes to prepare the record. The HITECH Act changes these requirements for covered entities using EHR systems – it allows an individual to request that his or her record be produced in an electronic format and transmitted to a person designated by the patient. The HITECH Act further provides that the cost of producing an electronic copy of the record cannot be greater than the labor costs of responding to the request. The change by the HITECH Act clarifies that covered entities producing the record electronically cannot charge the same fee that they would if producing the record in a non-electronic format (which would cover the costs of copying and postage).

MINIMUM NECESSARY STANDARD

Requirements to disclose the minimum necessary PHI already exist in the Privacy Rule. The change to this requirement made by the HITECH Act is a direction to HHS to issue guidance on what constitutes "minimum necessary" by August 17, 2010. This guidance will take precedence over the current regulations (at 45 C.F.R. § 164.514(d)(1)). Until those regulations are issued, however, covered entities must continue to adhere to the current regulations which require that uses and disclosures be limited to the "minimum necessary" to accomplish the stated purpose of the use or disclosure.

CONCLUSION

The HITECH Act made broad changes to several parts of the HIPAA Privacy and Security Rules. These changes will continue to have an impact on the procedures of health centers and other covered entities. However, their implementation is so far piecemeal, giving health centers time to adjust and implement the new requirements, yet leaving them without much guidance on the changes still yet to come. It is likely that the HITECH Act is just the beginning of a series of changes to laws that will adjust and accommodate the increasing role of information technology in the provision of health care.

SUMMARY OF STEPS TO TAKE TO COMPLY WITH THE UPCOMING CHANGES TO HIPAA

- Determine whether the Breach Notification Rule applies to your health center. If it does, draft and implement a policy and procedure that encompasses the health center's obligations under the Breach Notification Rule and begin training staff on the new policy and procedure.
- Amend your Business Associate Agreements to reflect that business associates are now directly responsible for compliance with HIPAA. If the health center is subject to the Breach Notification Rule, include provisions regarding the Business Associates' obligations with respect to compliance with the Breach Notification Rule.
- For health centers using electronic health records, change applicable policies and procedures to show that an individual requesting a copy of their record has a right to receive it electronically and if elected, the individual may be charged only for the cost of labor of retrieving the record.
- Stay current on updates from NACHC, HHS, and HRSA. The changes to HIPAA made by the HITECH Act are numerous and complicated. We have provided a summary of some of the most important changes, but this Issue Brief is not comprehensive.