

# Health Law ALERT

*Current legal insights for health care executives*

March 12, 2009

Julie A. Knutson, Editor

## *“D” is for Details: Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) Makes Significant Changes to HIPAA Privacy and Security Rules*

If you have tried to read a copy of the American Recovery and Reinvestment Act of 2009, and can't get beyond the “stimulating,” tongue-twisting names imbedded in the Act - such as the “Health Information Technology for Economic and Clinical Health Act” - you probably are not alone (some senators might not have read it either). One must sift through the massive bill to get to Subtitle D, Part I - “Improved Privacy Provisions and Improved Security Provisions.” Health care entities are just beginning to digest the significance of these provisions. There are still many debatable definitions and provisions, and the devil is certainly in the details. This article reviews key sections of the Act representing the most significant changes to the statutory and regulatory privacy and security provisions of HIPAA since the law's inception.

### **SEC. 13400 DEFINITIONS**

A few key new terms are included in the Act, such as “breach.” *Breach* is defined as the “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” This definition raises many questions – such as what is the standard for determining whether an unauthorized person would not reasonably have been able to retain such information? The answer will most definitely lie in technical solutions utilizing encryption and other forms of data security. The provision also excludes two circumstances from the definition of a breach: (i) improper access that is unintentional, in good faith and within the

**Find back issues of our newsletters and alerts at: [www.bairdholm.com/news-updates-newsletters.html](http://www.bairdholm.com/news-updates-newsletters.html)**

scope and course of employment and the information is not further accessed, used or disclosed; and (ii) inadvertent disclosures by a workforce member to another workforce member or business associate who makes no further disclosure of the information. The definition of breach becomes critical when reviewing the breach notification provisions discussed later in this article.

The Act also includes newly defined terms - Electronic Health Record, Personal Health Record and Vendor of Personal Health Record. These definitions will have increased significance for both privacy and security as stimulus money is distributed.

Effective Date: February 17, 2010, unless otherwise specified

#### **SEC. 13401 APPLICATION OF SECURITY PROVISIONS**

1. *Security Rule Applicable to Business Associates.* The provisions of this section of the Act extend the majority of the current HIPAA Security Rule requirements (physical, technical and administrative safeguards and required policies and procedures) to business associates. Any new provisions contained in the Act are also extended to business associates and must become part of the Business Associate Agreement with covered entities.

**Effective Date:** February 17, 2010

2. *Penalties Extend to Business Associates.* This provision expressly extends the penalty provisions of HIPAA to business associates to the same extent they apply to covered entities. Later sections of the Act significantly increase the amount of those penalties, discussed later in this article.

**Effective Date:** February 17, 2010

#### **SEC. 13402 NOTIFICATION IN THE CASE OF BREACH**

1. *New Term – Unsecured Protected Health Information.* Under the Act, covered entities are now required to notify each individual whose “*unsecured protected health information*” has been or is reasonably believed to have been used or disclosed as a result of a breach. It is yet to be determined what will constitute “unsecured protected health information” triggering the breach notification provision. The Act refers to future guidance in its definition of unsecured protected health information: “information that is not secured through the use of technology or other methodology specified by the Secretary...” This guidance must be issued by April 18, 2009. If guidance is not issued by such date, the default definition for *unsecured protected health information* is “protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals...” The new definition of breach discussed at the beginning of this article must also be applied, making the determination of whether there is a reportable incident very complicated. Keep in mind that many states have breach notification provisions as well, and to the extent those requirements are more stringent than those in the Act, the state provisions will apply.

**Effective Date:** 30 days after issuance of regulations – or if regulations not promulgated by April 18, 2009, default definition applies as of such date.

2. *Discovery of Breach.* Covered entities must notify individuals upon *discovery* of the breach, and business associates must notify the covered entity upon *discovery* of a breach. When is a breach considered

*discovered?* A breach is deemed discovered as of the first day on which such breach is either (i) known to such entity or business associate, including any person (other than the individual committing the breach) that is an employee, officer, or other agent of such entity or associate, or (ii) should have reasonably been known to such entity, business associate or employee/officer/agent. This new notification provision makes it absolutely critical that employees be sufficiently trained to recognize a potential breach and required to report to their supervisor or the privacy officer any information that would reasonably suggest a breach of information security. We have always recommended that this duty to report be included in your policies, but its importance is heightened by this new provision. Covered entities must rely on an educated workforce now more than ever.

**Effective Date:** Final regulations must be published by August 16, 2009; effective 30 days after final regulations published.

### 3. *Method of Notice* –

- Notification to individuals by direct mail. Individuals must be notified by first class mail at the last known address. Only if the individual has specified a preference for communication by e-mail can such communication serve as notice. If there is insufficient contact information to make direct written notice, a posting of such information must be made on the covered entity's web site home page or notice in major print or broadcast media that reaches the areas where individuals are likely to reside. If there is an imminent threat to the individuals because of the breach (determined by the covered entity), phone calls may also be made.
- Notification via media. In addition to

notification to the individual described above, if unsecured PHI of more than 500 residents of a State or jurisdiction is involved in the breach, notice also must be provided to prominent media outlets serving that area.

**Effective Date:** Final regulations must be published by August 16, 2009; effective 30 days after final regulations published.

4. *Reporting Breaches to HHS.* Covered entities must log each breach notification that is provided to an individual or through media outlets. If a breach notification is made that involves more than 500 residents, the covered entity must immediately notify HHS. If a breach notification involves fewer than 500 residents, the covered entity must maintain a log of each breach and annually submit the log to HHS.

**Effective Date:** Final regulations must be published by August 16, 2009; effective 30 days after final regulations published.

## **SEC. 13404 APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES**

This section of the Act has been the subject of many articles headlining that all privacy provisions are now extended to Business Associates. We say – hold the presses. This section provides that when a business associate obtains or creates PHI pursuant to a business associate agreement with a covered entity, the business associate may use and disclose such PHI only if the use or disclosure is in compliance with each requirement of the business associate contract requirements of HIPAA (164.504(e)). It does not say that business associates are subject to all provisions of the Privacy Rule. It may seem redundant to specify in the Act that business associates who have a contract with covered entities

must comply with the provisions of the Privacy Rule related to the business associate contract. What the Act does is change a business associate's obligations from being purely *contractual*, to now *statutory*. But, the underlying *obligation* is still only what is spelled out in the business associate agreement. The difference now is that the Act extends statutory penalties under the Social Security Act expressly to business associates. Business associates may now face civil and criminal penalties in addition to civil damages for breach of contract.

An additional obligation placed on business associates under this section of the Act is the requirement for monitoring the activities of the covered entity. The business associate will be in violation of HIPAA if the business associate knew of a pattern of activity or practice of the covered entity that constitutes a violation of HIPAA, unless the business associate takes steps to end the violation. If those steps are unsuccessful, the covered entity must terminate the contract or report the breach to the Secretary of HHS. This provision will place business associates in a difficult position with respect to monitoring the activities of those covered entities with whom they contract.

**Effective Date:** February 17, 2010

#### **SEC. 13405 RESTRICTIONS ON CERTAIN DISCLOSURES AND SALES OF HEALTH INFORMATION; ACCOUNTING OF CERTAIN PROTECTED HEALTH INFORMATION DISCLOSURES; ACCESS TO CERTAIN INFORMATION IN ELECTRONIC FORMAT**

1. *Requests for Restriction.* Under the current Privacy Rule, individuals are permitted to request a restriction on how

the covered entity uses or discloses the individual's PHI for treatment, payment or health care operations. Currently, the covered entity is permitted to deny any requested restrictions. The Act changes that, and instead requires a covered entity to accommodate an individual's request that his or her information not be disclosed to a health plan for purposes of payment where the PHI relates to a health care item or service for which the provider is "paid out of pocket in full." This provision will require covered entities to enhance procedures for patients who say at the time of service – "I do not want this information shared with my insurance company." While many providers have implemented procedures to comply with this request, it will be important to ensure that any future treatment for which the health insurer is the payor and has access to records, does not refer to information that is subject to the restriction.

**Effective Date:** February 17, 2010

2. *Minimum Necessary Standard* – The Act specifies that a covered entity is in compliance with the minimum necessary standard if it discloses only the information comprising a limited data set (a small subset of information defined in the current regulations) to the extent practicable, or if more information is needed by the covered entity, the minimum additional information necessary. The Act also requires HHS to provide further guidance as to what constitutes minimum necessary. Once guidance is published, the "limited data set or something more that is the minimum necessary" no longer applies and the new guidance becomes the standard. The Act also clarifies that it is the covered entity who determines what information is the minimum necessary to accomplish the intended purpose of a disclosure. Covered

entities will not be able to rely on others who request the information, even other covered entities, as being the minimum necessary. This will have an impact on provider-insurer exchanges. Exchanges for treatment continue to be exceptions from this rule.

**Effective Date:** February 17, 2010, as revised by guidance to be issued by August 16, 2010.

### 3. *New Rules on Accounting for Disclosures*

– The Act materially alters the obligation to account for disclosures. Under the current Privacy Rule, covered entities are not required to provide an accounting of disclosures for treatment, payment or health care operations. Under the Act, covered entities that use or maintain an electronic health record will be required to account for disclosures for treatment, payment and health care operations purposes made during the three year period prior to the request (current rule is 6 years for other disclosures). By the end of this year, HHS is required to adopt standards on accounting for disclosures, and within six months thereafter adopt regulations on what must be included in the accounting.

This section also permits covered entities to provide an accounting of its disclosures, and provide a list of all business associates of the covered entity who may have made further disclosures on behalf of the covered entity. We anticipate this section to be the subject of much controversy as covered entities could have hundreds of business associates and an individual could be required to query each business associate to get the complete list of disclosures. A covered entity can choose to obtain the information from its business associates and provide a complete report to the individual. Business associate agreements will need to address how this situation will be handled.

**Effective Date:** The deadline for complying with this accounting requirement hinges on the date on which covered entities began using an electronic health record. If a covered entity acquired an electronic health record prior to January 1st of this year, the requirement for an accounting applies to disclosures made on or after January 1, 2014. If a covered entity acquires an EHR after January 1, 2009, the accounting requirement applies to disclosures on or after the later of January 1, 2011 or the date it acquires an electronic health record. Due to the much shorter deadlines for those who do not already have an EHR, the ability to track and log disclosures for treatment, payment and health care operations will need to be part of the RFP specifications for entities as they acquire EHR systems. Note that the Act permits the Secretary to extend the 2011 deadline for current EHR users to no later than 2016 and new EHR users to no later than 2013.

4. *Sales of Electronic Records or PHI.* The Act imposes new limitations on covered entities and business associates with regard to exchanging PHI for direct or indirect remuneration. A covered entity or business associate may not receive anything in exchange for giving PHI unless the disclosure is:

- Pursuant to an authorization that notifies the individual that remuneration will be received;
- For permitted research and the remuneration reflects the costs of preparation and transmittal of the data for such research;
- For treatment – subject to any new HHS rules;
- In connection with the acquisition or merger of covered entities;

- In connection with business associate functions and the remuneration is tied to those functions;
- To an individual and the remuneration relates to fees for copying/summaries.

**Effective Date:** HHS must publish regulations by August 17, 2010; effective date is six months after regulations are published.

5. *Access to Records.* The Act requires covered entities that maintain an electronic health record to provide electronic copies of records to patients upon request. The fee for providing the electronic copy can be no more than the labor costs in responding to the request. This revises the current Privacy Rule that allows for a pass through of expenses – thus preventing covered entities from passing on any hardware/software costs through fees for medical record production. State law should be considered here before imposing fees. As this provision and others relating to individual rights (new accounting rights) become final, a covered entity must remember to amend its Notice of Privacy Practices and redistribute to address the change in practice.

**Effective Date:** February 17, 2010

**SEC. 13406 CONDITIONS ON CERTAIN CONTACTS AS PART OF HEALTH CARE OPERATIONS**

This section of the Act addresses marketing and fundraising communications. The first change is that a communication to an individual (without any direct or indirect payment to the covered entity or business associate) is not considered a health care operations activity of the covered entity unless the communication is: (i) about a health-related product or service that is provided by the covered entity; (ii) for treatment of the individual; or (iii) for case management or care coordination

for the individual or to direct the care or recommend other therapies or treatment settings.

If the covered entity or a business associate will receive remuneration in connection with the communication, the communication qualifies as a health care operations activity only if the communication: (i) is regarding a drug or biological currently prescribed and the payment amount is reasonable; (ii) is made pursuant to an authorization of the individual; or (iii) is made by a business associate of a covered entity pursuant to an authorization.

This section also requires covered entities who send fundraising letters or other forms of communication to patients to provide a clear and conspicuous notice of the opportunity for the recipient to opt out of receiving any further communications. The opt out is treated as a revocation of authorization – which has the effect of a covered entity not being able to condition treatment on the individual not opting out.

**Effective Date:** February 17, 2010.

**SEC. 13408 BUSINESS ASSOCIATE CONTRACTS REQUIRED FOR CERTAIN ENTITIES**

This section of the Act imposes the requirement of business associate contracts on organizations who provide data transmission of PHI involving routine access to such PHI. Examples provided include Health Information Exchange Organizations, Regional Health Information Organizations and E-prescribing Gateway. Vendors of Personal Health Records also become business associates of the covered entities offering the services of such vendor.

**Effective Date:** February 17, 2010

## SEC. 13409 CLARIFICATION OF APPLICATION OF WRONGFUL DISCLOSURE CRIMINAL PENALTIES

This section expressly extends criminal penalties to wrongful disclosures by *any person* (including *employees of covered entities*) if the information was obtained from a covered entity without authorization. It is believed that this section is intended to “clarify” an earlier Department of Justice memorandum that opined that only covered entities (not individual employees) could be subject to criminal penalties. Despite that memo, many employees of covered entities were prosecuted under related statutes or under aiding and abetting theories. This provision gives clear and direct authority for the government to impose criminal penalties on employees (and any other person) if the information was obtained from a covered entity without authorization. It also provides covered entities with a stronger argument to retrieve PHI from employees who take it improperly – and it gets everyone’s attention during early morning training sessions!

**Effective Date:** February 17, 2010

## SEC. 13410 IMPROVED ENFORCEMENT

1. *Violations due to Willful Neglect.* This section provides that violations by covered entities due to willful neglect are subject to civil monetary penalties (CMPs). HHS must investigate any complaints of violations due to willful neglect. We anticipate this section to have a significant impact in enforcement – including application to covered entities who fail to monitor actions of employees.

**Effective Date:** Applies to penalties imposed on or after February 17, 2011. HHS is required to publish regulations not

later than August 17, 2010.

2. *Distribution of CMPs Collected.* While not getting much attention, this provision of the Act could have significant impact. The Act provides that CMPs collected for violations of privacy and security provisions shall be transferred to the Office for Civil Rights (OCR) – to fund further enforcement. Importantly, this section also requires the Government Accounting Office to issue a report by August 17, 2010 that includes a methodology *for providing a percentage of any CMPs or settlements to the individuals who were harmed by the violations*, and requires HHS to adopt regulations within three years thereafter, implementing a methodology for doing so based on GAO’s recommendations. This section could have ramifications for covered entities as individuals now have an incentive to report actual or perceived violations to OCR in the hopes that they can recover any CMPs collected. Currently no private right of action exists to bring suit against covered entities for violation of HIPAA. This quasi *qui tam* provision could result in an increase of complaints filed with OCR as individuals will have limited expense while the government investigates the complaint and potential financial rewards.

**Effective Date:** GAO to issue report by August 17, 2010; HHS to issue regulations within 3 years thereafter.

3. *Increase in Civil Monetary Penalties.* This section is the teeth of the Act. This section provides for a tiered increase of civil monetary penalties (CMPs) up to a maximum of 1.5 million dollars depending upon aggregating factors. Penalties are tiered as follows:

- For violations where the person did not know and by exercising reasonable diligence would not have known of the violation:

No Penalty – OCR may, in its discretion, impose corrective action without a penalty. If CMPs are imposed, must meet statutory penalty tiers.

Minimum - \$100/violation up to \$25,000 for identical violations/year

Maximum - \$50,000/violation up to \$1.5 million for identical violations/year

- For violations due to reasonable cause and not to willful neglect:

Minimum - \$1,000/violation up to \$100,000 for identical violations/year

Maximum - \$50,000/violation up to \$1.5 million for identical violations/year

- For violations due to willful neglect that ARE corrected:

Minimum - \$10,000/violation up to \$250,000 for identical violations/year

Maximum - \$50,000/violation up to \$1.5 million for identical violations/year

- For violations due to willful neglect that are NOT corrected:

Minimum - \$50,000/violation up to \$1.5 million for identical violations/year

**Effective Date:** February 17, 2009

#### 4. *Enforcement by State Attorneys General.*

The Attorney General of each State is now authorized to file suit in federal court for violations of HIPAA involving residents of the State. Damages may be awarded in the amount of \$100 per violation up to \$25,000 for identical violations during a calendar year. The court may award

reasonable attorneys fees to the State if it prevails in its suit. HHS may intervene in any such actions.

**Effective Date:** February 17, 2009

#### **SEC. 13411 AUDITS**

The Act requires HHS to conduct periodic audits to ensure covered entities and business associates are in compliance with the requirements of HIPAA. This is the first extension of potential audits to business associates.

**Effective Date:** February 17, 2010

The Act creates substantial new requirements for covered entities and their business associates that have a major impact on compliance activities. The penalties are significant, and enforcement will be increased. While other provisions of the Act provide incentives for the use of technology in the health information infrastructure, it is clear that privacy and security of such information will be front and center of the government's list of enforcement priorities. Some of the provisions of the Act are effective now – such as the increase in penalties. Others have one year prior to becoming effective and others have varying effective dates. Start planning now for implementing these new requirements and stay tuned as new regulations are on their way.

**Vickie Brady Ahlers**

**BAIRD HOLM<sup>LLP</sup>**  
ATTORNEYS AT LAW

#### **HEALTH CARE GROUP**

**Vickie Brady Ahlers**

402.636.8230

vahlers@bairdholm.com

**Alex (Kelly) M. Clarke**

402.636.8204

kclarke@bairdholm.com

**John R. Holdenried**

402.636.8201

jholdenried@bairdholm.com

**Andrew D. Kloeckner**

402.636.8222

akloeckner@bairdholm.com

**Julie A. Knutson**

402.636.8327

jknutson@bairdholm.com

**Barbara E. Person**

402.636.8224

bperson@bairdholm.com

*All attorneys are admitted to practice in Nebraska and Iowa.*

MEMBER  
**LEX MUNDI**  
THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

*Health Law Advisory* is intended for distribution to our clients and to others who have asked to be on our distribution list. If you wish to be removed from the distribution list, please notify [healthupdate@bairdholm.com](mailto:healthupdate@bairdholm.com).

**BAIRD HOLM LLP**

1500 Woodmen Tower

Omaha, NE 68102

402.344.0500

402.344.0588

[www.bairdholm.com](http://www.bairdholm.com)

©2009 Baird Holm LLP