Stimulus Bill Creates New Security and Privacy Challenges for Health Plans and Providers

Kibble & Prentice
A USI Company

Kibble & Prentice
A USI Company

Stimulus Bill Creates New Security and Privacy Challenges for Health Plans and Providers

H.R. 1, the American Recovery and Reinvestment Act of 2009 ("the Act"), passed the U.S. House of Representatives on February 13, 2009, by a vote of 246-184. Later that day, the Senate also passed the bill by a vote of 60-38. The President signed the bill on February 17, 2009.

This bill is a $780 billion package, with roughly 35% of the package devoted to tax cuts (mostly for 2009) and the rest to spending intended to occur in 2009 and 2010. Congress slipped major changes to the Health Insurance Portability and Accountability Act (HIPAA) into the Act that will have serious implications for healthcare providers. These changes, which are described below, alter the privacy and security rules under HIPAA, and increase enforcement and penalties for noncompliance.

RULES APPLY DIRECTLY TO BUSINESS ASSOCIATES INDIVIDUALLY

Before the Act

Only covered entities (including health plans and providers) were subject to the requirements of the HIPAA Privacy and Security Rules [(1) the administrative safeguards contained in 45 C.F.R. 164.308, (2) the physical safeguards contained in 45 C.F.R. 164.310, (3) the technical safeguards contained in 45 C.F.R. 164.312, and (4) the policies, procedures and documentation requirements contained in 45 C.F.R. 164.316]. Those assisting covered entities, known as business associates, were not directly subject to the Privacy and Security Rules. Instead, the covered entity was required to contract with the business associate to make sure that the health information to which the business associate had access was protected.

After the Act

The HIPAA privacy and security standards, as well as the civil and criminal penalties for violating those standards, now apply directly to business associates – individuals and entities that use, disclose or receive individually identifiable health information for or on behalf of current covered entities.

ENHANCED ENFORCEMENT PROVISIONS

Before the Act

HHS was authorized to conduct audits of HIPAA privacy and security compliance.

After the Act

In August of 2009, it was announced that the U.S. Office for Civil Rights (OCR) shall now conduct periodic audits to ensure compliance with HIPAA. (This was formerly conducted by the U.S. Department of Health and Human Services.) OCR is required to investigate possible violations if it is indicated that the alleged violation was possibly due to willful neglect. Further, OCR is required to impose civil penalties for violations due to "willful neglect." State Attorneys General are authorized to bring a civil action against individuals who violate the HIPAA privacy and security standards, in order to enjoin further such violation. Civil penalties increase to amounts ranging from $100 to $50,000 per violation with maximum penalties for additional violations in any one year ranging from $25,000 to $1,500,000.

The OCR is also able to issue subpoenas requiring the attendance and testimony of witnesses and the production of any evidence that relates to any matter under investigation or compliance review for failure to comply with certain requirements. They are also able to make exception determinations, under section 1178(a)(2)(A) of the Social Security Act, when provisions of state laws are contrary to Federal standards and are not preempted by Federal standards.

As well, the OCR will also audit groups of HIPAA-covered entities to ensure they are complying with the law.

BREACH NOTIFICATIONS

Before the Act

The HIPAA regulations did not directly require covered entities to notify HHS or individuals of a breach regarding the privacy or security of their protected health information (PHI). Whether notification was to be made was part of the covered entity's analysis of how to mitigate the breach and to adjust procedures to prevent its recurrence.

After the Act

Every covered entity must to notify a person when there is a "breach" of that person's PHI. In addition, the covered entity is required to keep a log of such breaches and submit the log annually to HHS. The notification to the individual must be made without unreasonable delay, but always within 60 days of discovery of the breach.

Further, any case in which 500 or more persons are affected by a breach, the covered entity must notify HHS or OCR immediately and provide notice to "prominent media outlets" in the area. Reported breaches of this magnitude will be posted on the HHS or OCR website for public viewing.

Notification of a breach must be by letter sent via first class mail to the affected person's last known address, or where a preference is stated, by electronic mail. If the covered entity does not have sufficient contact information then a substitute form of notice is to be provided, which, if more than 10 individuals are involved, may include posting on the covered entity's website or notice in major print or broadcast media. The covered entity must include a toll-free telephone number to call for information about the breach.

©2009 Kibble & Prentice Holding Company, All rights reserved.

If a possibility of imminent misuse of the PHI exists, then notification should be by telephone or other appropriate means.

Notification of even unintentional disclosures is required unless such disclosure is to an individual who is authorized to access health information at the same facility.

"Unsecured" PHI generally means information that is not encrypted or secured in such as manner as to make it unreadable to an unauthorized person. HHS issued guidance on the meaning of "unsecured" on April 17, 2009.

RIGHTS OF INDIVIDUALS

Before the Act

Individuals had a right to receive an accounting of disclosures of their PHI made by the covered entity over the prior six years, other than disclosures made to carry out treatment, payment, or healthcare operations of the covered entity.

After the Act

This right is expanded by providing that the exception for disclosures made to carry out treatment, payment, or healthcare operations does not apply to disclosures made through an electronic health record. Covered entities must track disclosures of electronic medical records made for treatment, payment and healthcare operations and provide an accounting to patients of such disclosures on request. This accounting of disclosures of electronic medical records must include disclosure for the period of three years prior to the date on which the accounting is requested.

Before the Act

Use or disclosure of PHI was limited (in most cases, but not all) to that which is minimally necessary.

After the Act

The covered entity must limit all of its uses, disclosures, or requests for PHI to that which is minimally necessary or contained in a limited data set.

Before the Act

An individual could ask for a restriction on the uses or disclosures of PHI by the covered entity, but the covered entity did not have to comply.

After the Act

If an individual requests a restriction on disclosures of PHI, the covered entity is required to comply if: (1) the individual requests a restriction on the disclosure to a health plan for payment or healthcare operations purposes and (2) the PHI pertains solely to services for which the individual has paid the provider out of pocket in full.

Before the Act

An individual has the right of access to his or her PHI contained in traditional medical records (45 C.F.R. 164.524).

After the Act

The right of access is expanded to allow an individual to request PHI in an electronic format and to direct it to be sent to another designated person or entity. The covered entity may impose a charge for providing an electronic copy. However, the charge may not exceed the covered entity's labor costs in responding to the request for the electronic copy.

EFFECTIVE DATES

Most Provisions of the Act	February 17, 2009
Notice of Breach	Effective for breaches discovered on or after thirty (30) days after the publication of the regulations
Expansion of Security and Privacy Rules to Business Associates	February 17, 2010
New Requirement to Comply With Requested Restrictions	February 17, 2010
New Access Requirements For Covered Entities Using Electronic Medical Records	February 17, 2010
Requirements on Accounting for Disclosures of Electronic Medical Records	January 1, 2014 for electronic medical records created prior to January 1, 2009 January 1, 2011 for electronic medical records created after January 1, 2009
Increased Penalty Amounts	February 17, 2009
Authority for State Attorney General Enforcement	February 17, 2009
Other Enforcement Provisions	Various
Enforcement Delegated to OCR	July 27, 2009

©2009 Kibble & Prentice Holding Company, All rights reserved.

CONSIDERATIONS & IMPACT OF THE LAW

- Covered entities must review and revise their HIPAA privacy and security policies, as well as administrative materials, record retention policies, and training logs to comply with the new provisions.
- Covered entities will need to review their HIPAA privacy notices to reflect the new provisions.
- Covered entities should review their business associate agreements. Most agreements will need to be modified to reflect the new requirements.
- Covered entities and business associates must properly train any employees who have contact with PHI from the group health plan on the new standards.
- Business associates must, amoung other requirements:
  - Conduct an accurate an thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the business associates (per 45 C.F.R. 164.308(a)(l)(ii)).
  - Implement a security awareness and training program (per 45 C.F.R. 164.308(a)(5)).
  - Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users (per 45 C.F.R 164.310(c)).
  - Assign a unique name and/or number for identifying and tracking user identity (per 45 C.F.R. 164.312(a)(2)(i)).
  - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI (per 45 C.F.R. 164.312(b)).

MORE TO COME

Under the Act, HHS is required to promulgate new HIPAA regulations on a variety of topics, including rules that:

- Implement the new notification of breach requirements
- Define "minimum necessary"
- Describe what information shall be collected in regards to the accounting of disclosures of electronic medical records
- Implement the prohibition on the sale of information from electronic medical records and exceptions thereto
- Implement the mandatory HHS investigations and penalties for violations due to willful neglect, and
- Establish a methodology for distributing a percentage of collected penalties to persons harmed by violations.

Seth Shapiro, Senior Vice President, Risk Strategist
Kibble & Prentice Risk Strategies Group
(206) 441-6300
www.kpcom.com

Stimulus Bill Creates New Security and Privacy Challenges for Health Plans and Providers

IRS Circular 230 Disclosure: Kibble & Prentice Holding Co. and its affiliates do not provide tax advice. Accordingly, any discussion of U.S. tax matters contained herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone unaffiliated with Kibble & Prentice Holding Co. of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties. Also, the information contained in this brochure should not be construed as medical or legal advice and is intended for educational purposes only. Kibble & Prentice operates in the State of California under the name of Kibble & Prentice Holding Company dba Kibble & Prentice Insurance Agency (0E28835).

Kibble & Prentice
A USI Company

©2009 Kibble & Prentice, Proprietary and Confidential