

Healthcare Privacy and Security Policy: New Provisions in the 2009 Stimulus Package *for the*

Western States Health-e Summit

**Lisa A. Gallagher, BSEE, CISM, CPHIMS
Senior Director, Privacy and Security
lgallagher@himss.org
March 3, 2009**

Topic Overview

- **Privacy and Security Provisions**
 - Breach Notification
 - Accounting of Disclosures
 - Business Associates
 - Marketing/Sale of PHI
 - Access/Restrictions
 - Limited Data Set/Minimum Necessary
 - Enforcement/Penalties
 - PHRs (summary)
- **What's Next**
 - Guidance and Rulemaking

Breach Notification

- Establishes a federal security breach notification requirement for breach of protected health information
- Requires each individual be notified if their “unsecured” PHI is accessed, acquired or disclosed as a result of the breach
- Requires notification to Sec HHS and prominent media outlets if more than 500 individuals impacted
- Applies to PHR vendors

Accounting of Disclosures

- Gives patients the right to request an accounting of disclosures of their health information made through an EHR
- Secretary of HHS to promulgate regulations that take into account the “interests of individuals” in learning when and to whom their information is disclosed, the “usefulness” of the information to the individual, and the “cost burden” for such accounting

Business Associates

- Applies some HIPAA standards to Business Associates directly
- Ensures that new entities that were not contemplated when HIPAA was written (such as PHR vendors, RHIOs, HIEs, etc.) are subject to the same privacy and security rules as CEs by:
 - **requiring Business Associate contracts, and**
 - **treating these entities as Business Associates under HIPAA**

Marketing/Sale of PHI

- Provides new restrictions on marketing using PHI
 - Marketing Communications are not Health Care Operations (with some exceptions)
- Provides new restrictions on payment for PHI
 - prohibits a CE/BA from receiving remuneration in exchange for any PHI without a valid authorization from the individual (with some exceptions)

Access

- Provides an individual the right to have access to certain information about them in electronic format, for which the provider may charge a fee
 - gives individuals the right to receive an *electronic* copy of their PHI, if it is maintained in an electronic health record

Limited Data Set/ Minimum Necessary

- CEs should limit uses and disclosures to Limited Data Set, or if needed,
- Minimum Necessary
- Sender determines Minimum Necessary
- Secretary to issue guidance on what constitutes Minimum Necessary

Enforcement/Penalties

- Allows criminal penalties to apply to individuals
- Provides new system of civil monetary penalties
- Modifies distribution of certain civil monetary penalties collected
- Requires the Secretary to provide for periodic audits of covered entities and business associates
- Allows State Attorneys General to bring a civil action in federal court on behalf of the residents of their state

PHRs

- The term **“Personal Health Record”** means an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is *managed, shared, and controlled by or primarily for the individual.*
- the term **“unsecured PHR identifiable health information”** means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under section ...

New Provisions Applying to PHRs

- **New “Temporary Breach Notification” applies to PHR vendors not currently covered by HIPAA**
 - Applies to breach of unsecured PHI in PHR
 - Notify individual
 - Notification of FTC and Sec HHS
 - *Conf agreement: FTC sets regulations*
- **Business Associate Contracts Required for Certain Entities**
 - HIEs, RHIOs
 - PHR vendors that offer products through/for provider or plan

New Provisions Applying to PHRs - *Future*

- **Apply HIPAA to PHR Vendors?**
 - **Sec HHS (w/ FTC) study and report to Congress**
 - **which federal agency is best equipped to enforce new requirements**
 - **time frame for implementing regulations**

Guidance and Rulemaking

- Guidance
 - Breach
 - Minimum Necessary
- Rulemaking
 - Accounting of Disclosures
 - Sale of PHI
 - Marketing
 - Enforcement/Penalties

Upcoming HIMSS Events

- Complimentary webinar series on Economic Stimulus and impact on members (Feb/Mar)
- HIMSS09
 - April 4 – 8 in Chicago
 - Economic Stimulus track – 10 sessions
- HIMSS Virtual Conference & Exhibition
 - June 9 – 10
- National Health IT Week and Advocacy Day
 - September 21 – 25 in Washington, DC

Resources

- **One-stop shop on the ARRA**
himss.org/EconomicStimulus
- **Summary**
himss.org/content/files/HIMSSSummaryOfARRA.pdf
- **Analysis**
himss.org/EconomicStimulus
- **FAQs**
himss.org/EconomicStimulus/docs/HIMSS_FAQs_ARRA.pdf
- **HIMSS09 Sessions on ARRA**
himssconference.org/education/ESPSessions.aspx
- **HIMSS P&S Toolkit**
<http://www.himss.org/ASP/privacySecurityTree.asp?faid=78&tid=4>