

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

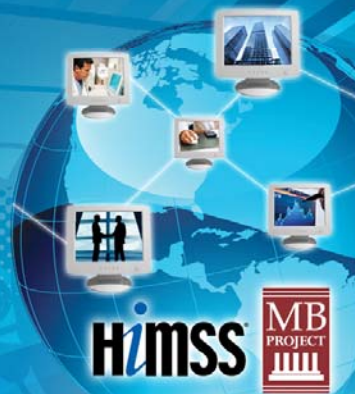
**Operationalizing Privacy &
Security**



EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

**American Recovery and
Reinvestment Act (ARRA)
Impacts on Privacy
and Security**

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



**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

American Recovery and Reinvestment Act

- H.R. 1, signed into law on February 17, 2009
- Aims to stimulate the economy through investments in infrastructure, unemployment benefits, transportation, education, and healthcare
- Title XIII – Health Information Technology for Economic and Clinical Health (HITECH) Act
 - Subtitle A – Promotion of HIT
 - Subtitle B – Testing of HIT
 - Subtitle C – Grants and Loans Funding
 - Provides nearly \$20 billion to assist in development of HIT infrastructure and to assist in adoption and use
 - Subtitle D – Privacy
- Title IV – Medicare and Medicaid HIT
 - Incentives for adoption and “meaningful use” of certified electronic health record (EHR) technology

**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

What ARRA Privacy and Security Provisions Attempt to Accomplish

- Broaden the scope of applicability for the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules to encompass business associates
- Provide transparency for breach victims
- Provides additional accounting of disclosure requirements
- Tighten restrictions on the use and disclosure of protected health information (PHI) – marketing and sales
- Strengthen consumers’ privacy rights
- Strengthen compliance oversight, enforcement, and sanctions for violations

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

ARRA Privacy and Security Provisions

- Breach Notification
- Accounting of Disclosures
- Business Associates
- Marketing/Sale of PHI
- Patient Access
- Limited Data Set/Minimum Necessary
- Enforcement/Penalties
- PHRs
- Other factors
 - Guidance and Rulemaking

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

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 – Report to FTC
- Interim Final Rule published – effective Sept. 23, 2009
 - Includes “Harm Provision”

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Breach Notification - Implications

- Establishes law requiring notification breach of un-protected health information (PHI) *at federal level*
- Formally defines “Breach”
- Defines “Unsecured” and provides a Safe Harbor when secured
- Provides guidance specifying protection technologies and methodologies that effectively render PHI unusable, unreadable, or indecipherable
- Notification requirement (to individual, HHS, and public) will heighten attention to healthcare security breaches
- Healthcare industry will need to focus on issues around security breaches – prevention, detection, assess harm, notification process

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

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

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Accounting of Disclosures - Implications

- Extends accounting of disclosures requirement *beyond HIPAA* – now includes disclosures that are made for treatment, payment or health care operations (commonly called “TPO.”)
- Regulation due from HHS by June 30, 2010

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Business Associates

- Applies some HIPAA standards to Business Associates directly (HIPAA Security and some Privacy)
- 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**

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Business Associates - Implications

- By extending HIPAA's scope to include BAs, new provisions expose BAs to direct regulation by the Department of Health and Human Services (HHS) and oversight and enforcement by the Office of Civil Rights (OCR)
- Increases business risk for BAs, while reducing risk for covered entities (in theory)
- Both BAs and the individuals who support these contracts are subject to civil and criminal penalties

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

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)

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Marketing/Sale of PHI - Implications

- Prohibits many types of marketing to patients that are common today
- Aims to put a serious dent in the health data “secondary market”

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

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

Access - Implications

- Covered entities must put in place new administrative processes to accommodate these requests from patients.

Limited Data Set/Minimum Necessary

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

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

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
- Moves HIPAA Security Enforcement to HHS' Office of Civil Rights (OCR)
- Allows State Attorneys General to bring a civil action in federal court on behalf of the residents of their state

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Enforcement/Penalties - Implications

- **Security and Privacy enforcement now centralized in the OCR**
- **Increased enforcement of the HIPAA rules (essentially none previously)**
- **Heightened efforts to pursue and penalize individuals and employers**
- **Increased enforcement in situations where a violation clearly occurred, even though limited harm resulted (such as "snooping" cases)**
- **Extent to which covered entities and business associates conscientiously attempt to comply with HIPAA rules to factor into enforcement and sanction decisions**
- **AG's – fear of politically motivated law suits**

**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

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
- **Business Associate Contracts Required for Certain Entities**
 - HIEs, RHIOs
 - PHR vendors that offer products through/for provider or plan

**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

New Provisions Applying to PHRs - Implications

- **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

EIGHTH NATIONAL MEDICAL BANKING INSTITUTE

The “ARRA Effect”

- Before ARRA, the Office of the National Coordinator (ONC) was an office established by Executive Order to oversee activities relating to the development of health information technology (HIT) standards
 - ARRA established the ONC as an office reporting to the Secretary HHS
- The standardization process included “acceptance” and (one year later) “recognition” of HIT standards, implementation specifications, and certification criteria, based on recommendations from the American Health Information Community (AHIC) Federal advisory committee (FACA)
 - ARRA established an infrastructure and set of processes for “adopting” standards, implementation specifications, and certification criteria, based on recommendations from the ONC
- The Health Information Technology Standards Panel (HITSP) developed, reviewed, and approved HIT specifications, which were recommended to AHIC
 - ARRA established two new FACAs – the HIT Standards Committee recommends standards, implementation specifications, and certification criteria, based on priorities established by HIT Policy Committee

EIGHTH NATIONAL MEDICAL BANKING INSTITUTE

FACAs – Contributions and Recommendations

- HIT Policy Committee recommended “meaningful use” goals, objectives, and measures that were incorporated into the Centers for Medicare and Medicaid Services (CMS) Incentive Program Notice of Proposed Rule Making (NPRM)
 - Recently added three new Workgroups – Privacy and Security Policy, Strategic Planning, and NHIN – all of which are expected to be key areas of focus in 2010
- HIT Standards Committee recommended the standards, implementation specifications, and certification criteria that were incorporated into the Interim Final Rule (IFR)
 - Reviewing IFR and providing comments to ONC
 - Shifting focus to standards for 2013 and 2015
 - Anticipating that new standards will be needed to support policy priorities from Policy Committee (especially in privacy and security, and health exchange/NHIN)

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Resources

- **ONC: <http://healthit.hhs.gov>**
- **CMS: www.cms.hhs.gov**
- **HIMSS: One stop for all ARRA information**
 - **www.himss.org/economicstimulus**
 - Summary, Analysis, FAQs
 - RSS Feed, Social Media
 - Tools & Resources

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Examples of Tools & Resources at www.himss.org/economicstimulus

- **HIMSS10 Sessions on ARRA**
himssconference.org
- **EHR Best Practices**
himss.org/davies/resources.asp
- **Privacy & Security Toolkit**
himss.org/ASP/privacySecurityTree.asp?faid=78&tid=4
- **Selecting the Right EMR Vendor & Online Buyers Guide**
himss.org/content/files/SelectingEMR_Flyer2.pdf
onlinebuyersguide.himss.org/
- **CDS & MU Home Page**
himssclinicaldecisionsupportwiki.pbworks.com/CDS-and-Meaningful-Use-Home-Page

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Thank You!!
- QUESTIONS?
- My contact information:

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