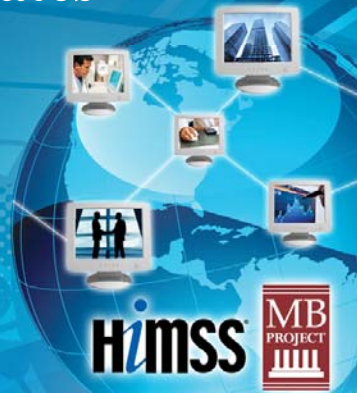


EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

**Privacy & Security
Issues and Updates**



EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

**Health Information Security
Under ARRA**
Embracing Enhanced Responsibility

Presented by:

Richard D. Marks
Co-Founder and President
Patient Command, Inc.
and

Mary Rita Hyland
Assistant Vice President Regulatory Affairs
The SSI Group, Inc.



EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- **ARRA changes the rules for security of health information in the U.S.**
 - Modifies HIPAA security (more below)
 - Imposes new security requirements for HIPAA covered entities and their business associates
 - Imposes security requirements for Personal Health Record (PHR) systems and others not covered by HIPAA
 - Enacts a new regime for breach notification
 - Emphasizes enforcement at the federal and state levels, including required federal investigations and enforcement by state attorneys general and whistleblowers

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Hierarchy of diligence and culpability
 - Reasonable diligence and would not have known
 - Reasonable cause and not willful neglect
 - Willful neglect (and corrected or not corrected)
- Increased, tiered civil and criminal monetary penalties – top is \$50,000 per violation, with annual limit of \$1,500,000

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Civil and criminal liability (i.e., prison terms) for individuals as well as organizations
- Breach notification for unsecured information (in effect, requires NIST – described encryption)

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- **Integrated health information security is inherent in ARRA**
 - Sections 13401, 13404 – references in business associate contracts now, by law, apply mutually (both ways) to covered entities and business associates
 - Requires reassessment of what business associate agreements mean for both CEs and BAs – both as to responsibilities for, and liabilities related to, security
 - This is not just a legal analysis – it requires reassessing business processes and technology
 - This is costly – and no one wants to hear that
 - People have yet to focus on Sections 13401 & 13404

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- For banks that offer clearing services for health transactions, or for banks that are considering offering PHRs –
 - What is the relationship among ARRA/HITECH, HIPAA as amended by ARRA, and GLB?
 - What agencies have enforcement authority, and is it exclusive or overlapping?
 - What new liability and other risk management issues arise under the new combination of ARRA/HITECH/HIPAA and GLB?

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- **What does this mean for:**
 - Boards of directors?
 - Senior (C-suite) executives?
- Issues for public companies
 - Sarbanes-Oxley governance
 - Public company disclosure and accounting
- Practical consequences of transitioning from an era of subdued (read “non-”) enforcement to an era of enhanced enforcement
- Demands a different approach to security risk and response models – diligence is the goal

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Mary Hyland – IT and ARRA

- While ARRA modified the rules for security of health information, Clearinghouses were already complying with advanced directives based on their Electronic Healthcare Network Accreditation Commission certification and following National Institute of Standards and Technology (NIST) guidelines.

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- The Advanced Network Technologies Division of NIST works as a partner with the information technology industry to improve the quality, reliability, resilience, robustness, manageability, security and interoperability of networked systems.
- The Information Access Division provides evaluations, measurements and standards to advance technologies dealing with access to multimedia and other complex information.

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Software is developed utilizing NIST guidelines for accessing unstructured, digital multimedia and other complex information, including text, web pages, images, video, voice, audio, and graphics (both 2-D and 3-D).
- While HITECH broadened the category of health information that must be protected, software vendors and clearinghouses were already thinking beyond current regulatory guidelines to the future with new technology and outlining how we can protect against the development of new methods to breach the security of information within.

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Operationally ensuring compliance with HITECH's security and privacy provisions is, to a large degree, an IT function.
- The security rules established under HIPAA do not require any particular IT system or set of safeguards. HITECH does not impose specific mandates on private entities, either.
- The HITECH Act does, however, direct HHS to issue guidelines every year on the "most effective and appropriate technical safeguards" for carrying out HIPAA security standards.

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- While the word “encrypt” does not occur even once within ARRA , HHS guidance specifies that if encryption solutions are used that meet the minimum specified standards, then if PHI is encrypted using those solutions, and a security incident occurs in which an unauthorized individual gets his or her hands on the PHI file, it would not be considered as a privacy breach and the notification would not need to occur.

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Request for Restrictions – IT systems must be modified

- Individuals may request restrictions [with which the covered entity must comply] on disclosure of
- PHI to a health plan if the provider has been paid by the individual;
- Exceptions include disclosures required for treatment or required by law.
- Impact/Risk
- Flags for disclosure restrictions
- Process impacts

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Access to Medical Records or EHRs

- Individuals may request copies of records be provided in electronic format;
- Impact /Risk
 - EHRs technology
 - Definition of “electronic” (e.g., CD, DVD, etc)
 - Potential breach risks if not tightly controlled

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Recommended Steps

- If you have not done so already, conduct organizational awareness training on ARRA and HITECH
- HIPAA and HITECH gap analysis in your organization should identify products, procedures, and services that need to be updated or modified
- Identify and coordinate technical or product updates
- Coordinate and implement policy and procedure updates
- Then conduct an audit to assess compliance.

**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

MBProject Gold Seal for Medical Banking Groups

- MBProject's Gold Seal sets a new standard for the banking and financial services industry in the critical area of data privacy and security.
- The Gold Seal assures customers that they are receiving services that have been recognized as meeting the highest standards of data privacy and security compliance mandated under banking and healthcare regulations, including HIPAA.

**EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE**

Service areas that may achieve a Gold Seal include

- **Bank-based electronic health data transaction services**
- **New lockbox programs that offer health data management programs**
- **New credit/debit card programs that link banking and healthcare systems**
- - **Banks/FIs that offer electronic and/or personal healthcare records**
- **Banks that offer account-based healthcare plans (HSAs)**
- **New healthcare ERA/EFT service areas**
- **Specialized healthcare lending programs**
- **Medical statement/print centers**
- - **Other service areas that combine banking and healthcare systems**

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

- Next we would like to poll the audience for the Privacy & Security section of the Gold Seal self-assessment program for the Medical Banking Groups.
 - Open Discussion

EIGHTH NATIONAL
MEDICAL BANKING INSTITUTE

Mary Rita Hyland, AVP
Regulatory Affairs
The SSI Group, Inc.
1-800-880-3032 ext 1120
Mary.Hyland@ssigroup.com
www.thessigroup.com

Richard D. Marks
Patient Command, Inc.
McLean, Virginia
richardmarks@earthlink.net
www.patientcommand.com