IACT Medical Trust

HIPAA Privacy Training

June 28, 2012

Jim Hamilton
(317) 684-5419
jhamilton@boselaw.com

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

HIPAA Overview

BOSE McKINNEY & EVANS LLP

ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

The Privacy Rule

- HIPAA Privacy Rule generally covers “protected health information” (“PHI”) transmitted or maintained in any form or medium (electronic or otherwise).
- These standards apply to four types of “Covered Entities”:
  - Health plans;
  - Health care clearinghouses;
  - Health care providers that conduct certain types of transactions in electronic form; and
  - Enrolled sponsors of the Medicare prescription drug discount card.
- Trustees of the IACT Medical Trust are entitled to access PHI in connection with plan operations.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Protected Health Information

- Protected Health Information (PHI) is individually identifiable health information that is maintained or transmitted by a Covered Entity, subject to certain exceptions.
- Employers often have access to and receive individualized health information about employees in the course of employment. However, this information is not PHI unless it is maintained or transmitted by a Covered Entity. For example, worker's compensation, LTD/STD, FMLA, ADA, and OSHA information maintained by an employer is not covered by the HIPAA Privacy Rule.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Core Requirement # 1: Use and Disclosure Rules

- Covered Entities are prohibited from using or disclosing PHI except as permitted under the Privacy Rule. It is permissible to disclose PHI for treatment, payment and health care operations. Further disclosures generally require an authorization.
- Many disclosures are subject to a "minimum-necessary standard." Under this standard, a Covered Entity must reasonably ensure that any PHI used, disclosed or requested is limited to the minimum information necessary to accomplish the intended purpose of the use, disclosure or request.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Core Requirement # 2: Individual Rights and Privacy Notice

- Under the Privacy Rule, individuals are granted certain rights with respect to their health information, including the right to:
  - Inspect and obtain a copy of their own PHI;
  - Amend or correct PHI that is accurate or incomplete;
  - Obtain an accounting of certain disclosures of their PHI that were made by Covered Entities;
  - Receive the notice of privacy practices required by the Privacy Rule;
    - Provided at time that individual enrolls in the medical plan. Triennial notification to participants of availability of notice.
  - Request additional restrictions on the use or disclosure of their own PHI.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Core Requirement # 3: Administrative Requirements

- The Privacy Rule also require Covered Entities to take the following actions to protect PHI:
  - Designate a Privacy Official;
  - Train workforces on privacy policies and procedures;
  - Establish appropriate safeguards to protect privacy of PHI;
  - Create system for individuals to lodge complaints;
  - Mitigate, to the extent practicable, any harmful effect that is known to the Covered Entity resulting from any use or disclosure of PHI;
  - Refrain from intimidating or retaliating against individuals or others for exercising their rights under the Privacy Rule.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Enforcement

BOSE McKINNEY & EVANS LLP

ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

HIPAA Enforcement

- The Office of Civil Rights of the Department of Health and Human Services (HHS) has received 68,410 complaints since enforcement began in April 2003.
- HHS imposed its first civil monetary penalty in January 2011 against Cignet Health Center.
- HHS has referred 499 cases to the United States Department of Justice for possible criminal prosecution.
- There have been at least 15 prosecutions under HIPAA, most of which involved actual or attempted identity theft or fraud.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

HHS Resolution Agreements

- HHS has entered into resolution agreements with four Covered Entities.
- In July 2008, HHS required a resolution agreement with Providence Health & Services to settle potential violations of the privacy and security requirements. Under the agreement, Providence agreed to pay $100,000 and implement a detailed corrective plan to appropriately safeguard electronic PHI.
- In January 2009, HHS required a resolution agreement with CVS Pharmacy. CVS was disposing of non-electronic PHI (such as labels from prescription bottles) in dumpsters that were potentially accessible to the public. CVS made payment of $2.25 million to HHS in accordance with the agreement.
- Most recent resolution agreements were with Massachusetts General Hospital, the University of California and the Alaska Department of Health and Social Services.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Health Information Technology for Economic and Clinical Health (HITECH) Act

BOSE McKINNEY & EVANS LLP

ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Overview

- HIPAA Privacy Rule initially effective April 14, 2003
- Heath Information Technology for Economic and Clinical Health (HITECH) Act included in federal stimulus passed in 2009
- HITECH allocates approximately $20 billion towards health IT infrastructure, industry standards, and incentives for health care providers and facilities to adopt electronic health record technologies.
- HITECH also made substantive changes to HIPAA Privacy Rule and Security Rule. Changes are generally effective one year from the date of ARRA enactment.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

HIPAA: Increased Penalties under HITECH

- Penalties for violations in which the individual does not know, the minimum penalty is $100 per violation (up to a maximum of $25,000 for identical violations during a calendar year).
- For violations due to reasonable cause, the minimum penalty is $1,000 per violation, with a cap of $100,000 for identical violations during the same year; the maximum penalty is $50,000 per violation, up to $1.5 million for identical violations during the same year.
- For violations due to willful neglect that are corrected, the minimum penalty is $10,000 per violation, with a cap of $250,000 for identical violations during the same year; the maximum penalty is $50,000 per violation, up to $1.5 million for identical violations during the same year.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

HIPAA: Expanded Enforcement under HITECH

- State Attorneys General now have the power to enforce HIPAA by bringing suit in federal court.
- The Secretary of the Department of Health and Human Services may bring both criminal and civil actions to enforce the HIPAA privacy and data security requirements.
- HITECH requires the Department of Health and Human Services to periodically audit Covered Entities and Business Associates to assess HIPAA compliance. Lengthy audit protocols were recently published.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

Breach Notification Requirements

- Covered Entities with “unsecured PHI” are required to timely notify individuals in the event of a breach. Business Associates with unsecured PHI have an obligation to notify the Covered Entity of any breach.
  - A breach is defined as an unauthorized acquisition, access, use or disclosure of PHI which compromises the use or disclosure of the PHI.
- HITECH includes specific content and timing requirements for notifications to individuals whose unsecured PHI was (or it is reasonably believed to have been) accessed, acquired or disclosed as a result of a breach.
- A notice must be immediately provided to the Secretary of Health and Human Services if 500 or more individuals are affected by the same breach.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP

New Business Associate Rules under HITECH

- As a result of HITECH, business associates are subject to direct regulation and enforcement under the HIPAA Privacy and Security Rules.
  - Business associates will have to review how they create, receive, maintain or transmit electronic PHI under these standards.
  - Business associates will have to maintain and retain written documentation of the policies and procedures implemented to comply with the HIPAA Security Rule.
  - If a business associate violates the HIPAA Privacy or Security Rules, then such business associate will be subject to civil and criminal penalties.
- Plan sponsors and Covered Entities should undertake a thorough review of business associate agreements and relationships with existing business associates.

BOSE McKINNEY & EVANS LLP
ATTORNEYS AT LAW

©2009 Bose McKinney & Evans LLP