Compliance Challenges for Researchers in the Post-HITECH World

N. Ajoy Mathew, J.D., M.H.S.
Associate Counsel, Research
Disclaimer

- This presentation and the analyses and opinions presented herein do not necessarily reflect the opinion, views, or analyses of the Children’s National Medical Center, the Children’s Research Institute, or its other affiliates or subsidiaries or the Directors, Officers, or employees thereof. The presentation is not and should not be construed as legal advice or be considered wholly accurate or complete for a general or specific purpose.
Overview

• The *Health Information Technology for Economic and Clinical Health (HITECH)* Act
  – Data Breach
  – Emerging Regulatory Landscape (New Civil Money Penalty Tiers)
  – Cases
  – Children’s National Policy and Procedure
  – Children’s National Resources
HITECH – Enactment & Purpose

• The Health Information Technology for Economic and Clinical Health (HITECH) Act, signed into law on February 17, 2009
  • Enacted as part of the American Recovery and Reinvestment Act of 2009
  • To promote the adoption and meaningful use of health information technology
  • Effective Purpose for Hospitals and Healthcare Institutions is to enhance enforcement of the HIPAA regulations
HITECH – Enactment & Purpose

• HITECH modified the HHS Secretary’s authority to impose civil money penalties for violations occurring after Feb. 18, 2009, significantly increasing the penalty amounts the Secretary may impose for violations of the HIPAA rules.
HITECH – Data Breach

• A “Data Breach” is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
**Exceptions to the definition of “breach”**

- Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate.
- In both cases above, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
Exceptions to the definition of “breach” (continued)

If the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information
HITECH – Data Breach Notification

• Data Breach Notification Requirement:
  – Covered entities and business associates must only provide the required notification if the breach involved unsecured protected health information
  – Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance
HITECH – Data Breach Notification

• The guidance document issued by HHS specifies:**
  – Encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals

**Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information
HITECH – Data Breach Notification

• HITECH and De-Identified PHI
  – De-identified information is not subject to HITECH or the provisions requiring protected health information (PHI) to be unusable, unreadable, or indecipherable to unauthorized individuals because once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, therefore, no longer subject to the HIPAA Privacy and Security Rules
  – Guidance not to be read as discouraging using of de-identified PHI
HITECH – Data Breach Notification

• Following a breach of unsecured protected health information, Covered Entities must provide notification of the breach to:
  – Affected Individuals
  – HHS Secretary
  – Media (certain circumstances)
  – Also: Business Associates must notify Covered Entities that a breach has occurred
HITECH – Data Breach Notification

• Notice to Individuals:
  – By first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically
  – Without unreasonable delay and in no case later than 60 days following the discovery of a breach
HITECH – Data Breach Notification

• Notice (to Individual) must include:
  • A description of the breach
  • A description of the types of information that were involved in the breach
  • The steps affected individuals should take to protect themselves from potential harm
  • A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches
HITECH – Data Breach Notification

• Notice (to Individual) (continued):
  • Contact information for the covered entity
  • Substitute notice provided via web posting or major print or broadcast media must include a toll-free number for individuals to contact the covered entity
HITECH – Data Breach Notification

• Notice to Media
  – For breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, the Covered Entity is required to provide notice to prominent media outlets serving the State or jurisdiction
    ▪ Press Release
    ▪ Without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice
HITECH – Data Breach Notification

• Notice to the Secretary of HHS
  – In addition to notice to Individuals and (as applicable), Media, Covered Entities must notify HHS
    ▪ HHS web site and submission of breach report form
    ▪ For breaches affecting 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach
    ▪ For breaches affecting fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis.
HITECH – Regulatory Changes

• Prior to the HITECH:
  – The HHS Secretary could not impose a penalty of more than $100 for each violation or $25,000 for all identical violations of the same provision
  – A covered health care provider, health plan or clearinghouse could also preclude the Secretary’s imposition of a civil money penalty by demonstrating that it did not know that it violated the HIPAA rules
HITECH – Regulatory Changes

• Post HITECH:
  – (Section 13410(d) of HITECH) strengthened the civil money penalty scheme by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision
  – A covered entity can no longer preclude the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery. The purpose of the foregoing provision is to encourage prompt corrective action
HITECH – Regulatory Changes

• Tiered increase in Civil Money Penalty (CMP):
  – Four categories of violations that reflect increasing levels of culpability
  – A maximum penalty amount of $1.5 million for all violations of an identical provision
### HITECH – New CMP Tiers

<table>
<thead>
<tr>
<th>Tiers of Violations</th>
<th>For violations occurring before 2/18/2009</th>
<th>For violations occurring on or after 2/18/2009</th>
<th>For violations occurring before 2/18/2009</th>
<th>For violations occurring on or after 2/18/2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>Up to $100</td>
<td>$100 - $50,000</td>
<td>$25,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>Up to $100</td>
<td>$1,000 - $50,000</td>
<td>All Identical Violations per Calendar Year</td>
<td>All Identical Violations per Calendar Year</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>Up to $100</td>
<td>$10,000 - $50,000</td>
<td>All Identical Violations per Calendar Year</td>
<td>All Identical Violations per Calendar Year</td>
</tr>
<tr>
<td>Willful Neglect – Not corrected</td>
<td>Up to $100</td>
<td>$50,000</td>
<td>All Identical Violations per Calendar Year</td>
<td>All Identical Violations per Calendar Year</td>
</tr>
</tbody>
</table>

---

HITECH – Regulatory Changes

• Covered entities and Business Associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach.

• Covered Entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures.
HITECH Cases

• Question:
  1. What are the reported major types of data breaches for Institutions reporting data breaches affecting more than 500 or more individuals?
HITECH Cases

• Answer to Q.1
  – Theft
  – Unauthorized Access/Disclosure
  – Improper Disposal
  – Loss
  – Hacking/IT Incident
  – Unknown
HITECH Cases

• Question:

2. What are the reported major locations of data breaches for Institutions reporting data breaches affecting more than 500 or more individuals?
HITECH Cases

• Answer to Q.2
  – Computer (Desktop/Laptop)/ Other Portable Electronic Device/Network Server
  – Paper
  – Electronic Medical Record
  – Email
  – Backup Disks
  – Backup Tapes
  – X-ray films
  – CDs
## HITECH Cases

<table>
<thead>
<tr>
<th>Type</th>
<th>Primary Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking/IT Incident</td>
<td>?</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>?</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>?</td>
</tr>
<tr>
<td>Loss</td>
<td>?</td>
</tr>
<tr>
<td>Theft</td>
<td>?</td>
</tr>
<tr>
<td>Unknown</td>
<td>?</td>
</tr>
</tbody>
</table>
# HITECH Cases

<table>
<thead>
<tr>
<th>Type</th>
<th>Primary Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking/IT Incident</td>
<td>Computer/ email/Network Server</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Computer</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>Paper/Other</td>
</tr>
<tr>
<td>Loss</td>
<td>Laptop/Other Portable Electronic Device</td>
</tr>
<tr>
<td>Theft</td>
<td>Laptop/Other Portable Electronic Device</td>
</tr>
<tr>
<td>Unknown</td>
<td>Other Portable Electronic Device/Backup Disks/Electronic Medical Records</td>
</tr>
</tbody>
</table>
HITECH Cases

• Question:

3. What are the approximate numbers of individuals affected in the largest reported data breach?

A. 5,000,000
B. 1,900,000
C. 1,700,000
D. 800,000
E. 300,000

See Reference 5.
HITECH Cases

• Answer:

3. What are the approximate numbers of individuals affected in the largest reported data breach?

A. 5,000,000 (actual - 4,901,432)(backup tapes)
B. 1,900,000
C. 1,700,000
D. 800,000
E. 300,000
HITECH Cases

• Question:
  4. What are the approximate numbers of individuals affected in a reported major data breach affecting a prominent Academic Medical Center?
   A. 5,000,000
   B. 1,900,000
   C. 1,700,000
   D. 800,000
   E. 300,000
HITECH Cases

• Answer:

4. What are the approximate numbers of individuals affected in a reported major data breach affecting a prominent Academic Medical Center?

A. 5,000,000
B. 1,900,000
C. 1,700,000
D. 800,000
E. 300,000 (actual 315,000) (backup discs)
Emory University – 315,000 Records

The Atlanta Journal-Constitution
Wednesday, April 18, 2012 | Posted: 7:00 p.m. Wednesday, April 18, 2012

Patient data missing for 315,000 Emory patients
Emory Healthcare said it cannot locate 10 computer discs containing personal and health information of 315,000 patients. Leak of Emory patient records could affect thousands
By Carrie Teegardin

The Atlanta Journal-Constitution

“Personal and health information for about 315,000 patients is missing, Emory Healthcare announced Wednesday. The hospital system has been unable to find 10 computer discs containing the data. The missing discs held information on all patients who had surgery at Emory University Hospital, Emory University Hospital Midtown and The Emory Clinic Ambulatory Surgery Center between September 1990 and April 2007. The discs contained protected health information, including patient names, along with the diagnosis, the name of the surgical procedure and the surgeon. Approximately 228,000 of the patient records also included Social Security numbers. "We sincerely regret that this incident has occurred and we want to assure our patients that we are committed to safeguarding their personal information," John T. Fox, president and CEO of Emory Healthcare, said at a press conference. Emory has no evidence that any information contained on the discs has been misused. Emory is sending letters to affected patients and offering them free identity protection and credit monitoring services. An investigation is ongoing to try to determine what happened to the discs. It's not certain that the information was stolen, Fox said. It could simply have been misplaced. The discs were removed sometime between February 7 and February 20, the investigation has determined..."
Other Legal Responses/Actions

• Audit
• Corrective Action
• Fines
• State Attorney General Actions
• Class Actions
Children’s National Medical Center

• Program, Policy and Procedure & Resources
  – Compliance Program – Training, FAQ, BAA Agreement
  – Subject Privacy & Confidentiality of Data
  – Storage and Retention of Research Data and Informed Consent Documents
  – Information System Security
  – CNMC Code of Conduct
Children’s National Medical Center

• Program, Policy and Procedure & Resources (continued)
  – Retention, Off-site Storage and POLICY: CH:A:33P;Destruction of Documents
  – Legal Department
  – Children’s National Staff and Researchers
References (Slides 3-34)


2. 45 CFR Parts 160 and 164; Modifications to the HIPAA Privacy, Security, Enforcement, and Breach; Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule; Federal Register, Vol. 78, No. 17 at 5566 (Jan. 25, 2013).

3. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information.


Children’s National Medical Center

Ajoy Mathew, J.D., M.H.S.
Associate Counsel, Research
Acting Director of Intellectual Property
Children’s National Medical Center
Direct: 202 476 3226
Legal Department: 202 471 4860
Amathew@cnmc.org

Thank You