Emerging Issues In Health Care Technology Part II: Privacy And Security

Presenters:

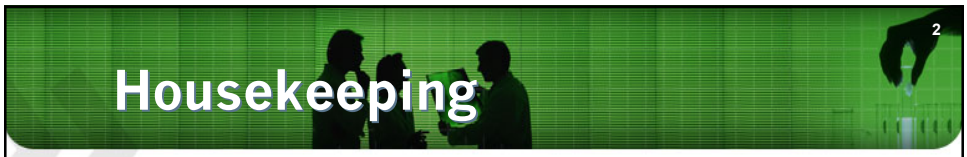
Lisa J. Acevedo, Partner, Health Care Industry Team, Foley

Shirley Morrigan, Partner, Health Care Industry Team, Foley

David Anderson, Associate Counsel, IT, Catholic Health Initiatives

Friday, October 24, 2008
11:30 a.m. – 12:30 p.m. CT

FOLEY
FOLEY & LARDNER LLP



Housekeeping

- We will take questions throughout the program via the Q & A tab located on your menu bar at the top of your screen and live questions at the end of the program
- Foley will apply for CLE credit after the Web conference. If you did not supply your CLE information upon registration, please e-mail it to mlopez@foley.com
- Today's program is being recorded and will be available on our Web site
- For audio assistance please press *0
- For full screen mode, go to "View" on your toolbar and select "Full Screen" or press F5 on your keyboard

HIPAA Enforcement Trends

HIPAA Enforcement Trends

- Privacy: 8132 Complaints in 2007; up from 7332 in 2006
  - 2007 top 5 issues in those investigated cases that were closed with corrective action
    - Impermissible uses and disclosures
    - Safeguards
    - Access
    - Minimum necessary
    - Notice

HIPAA Enforcement Trends

5

- Privacy Enforcement Trends: Top 5 Issues
  - #s 1-4 have been the same since 2003
  - # 5 has varied – 2006 it was "complaints to the CE"
  - Review of case examples
    - Many involved employee errors
    - Several were "wrongful" access, e.g., hospital supervisor accessing employee's medical record; nurse accessing ex-husband's medical record

HIPAA Enforcement Trends

6

- Examples of Corrective Action by OCR in 2007
  - Training
  - Revised policies and procedures
  - Counseling and disciplinary action for employees
  - Apology letters to patients
  - Out of 18 cited examples, no monetary penalties by OCR
    - 1 case – monetary settlement under state law

HIPAA Enforcement Trends

7

- Key Enforcement Event in 2008
  - Providence Health Resolution Agreement and Corrective Action Plan with HHS
    - Laptops, back-up tapes and other electronic media with unencrypted E-PHI were removed from premises and lost or stolen
      - 386,000 patients affected

HIPAA Enforcement Trends

8

- Providence Resolution Agreement and Corrective Action Plan
  - Providence notified affected patients per its state notification law and reported to HHS
    - Joint OCR/CMS investigation
      - OCR: Privacy → Safeguards
      - CMS: Security → Physical, Administrative and Technical Safeguards

HIPAA Enforcement Trends

9

- Providence Resolution Agreement and Corrective Action Plan
  - $100,000 "resolution amount" to HHS – not a civil monetary penalty
  - Corrective Action Plan
    - Revise policies and procedures to address encryption of E-PHI transported or stored off-site
    - Training, audits, site visits
    - Submission of compliance reports to HHS for 3 years

HIPAA Enforcement Trends

10

- Potential Drivers of the Resolution Agreement
  - Agencies were receiving negative publicity for lack of enforcement efforts with "teeth"
    - Viewed as especially problematic in light of drive to EMRs and interoperability
  - Escalation of security breaches, losses and theft of E-PHI and fears of identity theft
    - Highly publicized breaches, including the E-PHI of celebrities

HIPAA Enforcement Trends

11

- What Does the Resolution Agreement Signal
  - Increased focus on Security Rule Compliance and measures to prevent security incidents and unauthorized access to E-PHI
    - Continuation of CMS "on-site assessments" of Security Rule Compliance (Piedmont)
      - **OIG FY 2009 Work Plan** targets CMS' medical identity theft deterrence measures. Also targets security controls for portable devices implemented by hospitals and Medicare/Medicaid contractors
  - More stringent enforcement and payments

HIPAA Enforcement Trends

12

- Enforcement Drivers
  - Medical Identity Theft
    - Said to be the fastest growing form of identity theft
    - Theft could be facilitated by EMR Systems
      - e.g., rogue employees copying patient information onto thumb drives and selling
    - Possible legislation to come

EHR 2.x

Electronic Health Record Security in an Evolving World

EHR 2.x

- Current State of EHR Security
  - A typical conversation between departments:
    - The legal department says that our EHR system may not meet legal requirements
    - Ask them again – or ask a different attorney; maybe they will change their mind or we will get a different answer

- Practical Contractual Considerations for Securing an EHR system:
- Legal Landscape-
  - HIPAA
  - State Laws
  - FTC Red Flags Rules
  - Contractual Requirements (RHIOs, RHINs)

- Aspects of Security:
  - Authentication of Patients at the Point of Entry into the EHR System
    - Some new systems on the market permit self-directed patient registration
    - Proper documentation to verify identity of patients at registration or treatment
    - More difficult in emergent or urgent settings

- Contractual Considerations in EHR Agreements
  - Involve Key Stakeholders that analyze security issues during contract development and negotiation
  - Incorporate Partnering Principles that give the licensee the ability to influence product development and that address software modifications required as a result of legislative or regulatory changes

- Include Contractual Provisions Regarding CCHIT Certification:
  - Sample Language -
    - CHHIT Certification. [Vendor] represents and warrants to [Licensee] that it has received as of the Effective Date and shall maintain in effect at all times during the term of the Agreement electronic health record certification from the Certification Commission for Healthcare Information Technology, or any successor or replacement agency or authority

- Include Contractual Provisions Addressing Security Compliance:
  - [Vendor] will maintain and enforce physical security procedures with respect to access and maintenance of [Licensee Data] that provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of [Licensee Data]

- Anti-Hacker Standard Language:
  - [Vendor] will take all reasonable measures to secure and defend its location and equipment against "hackers" and others who may seek, without authorization, to modify or access the [Vendor] systems or the information found in such systems
  - Include a clear obligation on the part of the [Vendor] to report any breach of security or unauthorized access

- Additional Contractual Considerations:
  - Ownership of Data
    - Define what constitutes Licensee Data and add requirements that it not be commercially exploited, sold or leased to third parties
  - Accessibility
    - Use language to require the Vendor to make any Licensee Data accessible to Licensee through the use of commercially available tools

- Other Practical Considerations:
  - Offshoring
    - Consider language to restrict offshoring such as requiring that all of the Vendor obligations be performed from locations or using employees or contractors situated within the United States and that Licensee Data not be transmitted outside of the United States
  - Software Modifications
    - Require Vendor (at its own cost) to continually update and develop the software to comply with all applicable regulatory requirements

Expansion of State IT Security Breach Laws to Medical Providers

23

- Newest
  - Nevada (10/08)
    - Requires encryption of personally identifiable data
      - Names and credit card numbers, if transmitted electronically
      - Includes health care providers

Expansion of State IT Security Breach Laws to Medical Providers

24

  - Massachusetts (1/09)
    - Encrypt sensitive data stored on laptops and other portable devices
    - Attorney General developing an enforcement policy
      - Liability in civil suits
  - California (1/1/08)
    - Privacy law applies to all companies that maintain medical information
    - Data breach notification includes electronic medical information

Expansion of State IT Security Breach Laws to Medical Providers

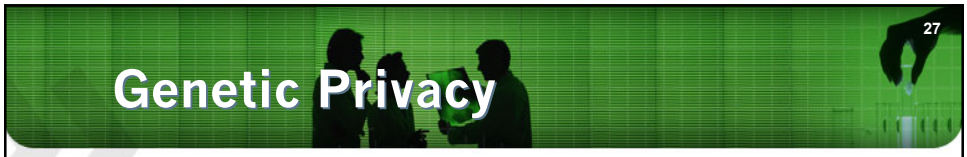
25

- Companies that do business in many states face a patchwork of state laws
- Earliest: protection of financial records/identity theft
- Mid: notification to consumer required in case of security breach
- New: protection of data
  - If electronic
  - Extending to health care
  - Healthcare identity theft [Red Flags]

Expansion of State IT Security Breach Laws to Medical Providers

26

- Security technology
  - Encrypted hard drives
  - Encryption software
- States/territories affected:
  - Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming



Genetic Privacy

27

- Federal Genetic Information Nondiscrimination Act of 2008 (GINA)

"GINA"

28

- GINA Provisions:
  - Generally: Prohibits employers and group health plans from discriminating based on "genetic information" and strictly limits the collection of such information
  - Acts as a floor of protection but does not preempt higher regulation under state law
    - 34 states have their own genetic information laws

- Important Definitions in GINA
  - "Genetic Information:" Information about
    - An individual's "genetic tests" (*i.e.*, analysis of DNA, RNA, chromosomes, proteins or metabolites that detect genotypes or chromosomal changes)
    - Genetic tests of the individual's family members

    - The "manifestation of a disease or disorder" in the individual's family members (not limited to hereditary conditions or to biological relatives)
  - "Family Members" include
    - Dependents
    - "Any other individual who is a [first-fourth degree] relative of the individual or such individual's dependent"
    - Applies to spouses, adopted children

Questions & Answers

Contact Us

Lisa J. Acevedo
Partner
Foley & Lardner LLP
321 N. Clark St., Ste 2800
Chicago, IL 60610
Tel: 312.832.4381
lacevedo@foley.com

David Anderson
Associate Counsel, IT
Catholic Health Initiatives
9780 S. Meridian Blvd., Ste. 300
Englewood, CO 80112
Tel: 720.875.7203
DavidAnderson@catholichealth.net

Shirley Morrigan
Partner
Foley & Lardner LLP
555 South Flower St., Ste 3500
Los Angeles, CA 90071
Tel: 213.972.4668
smorrigan@foley.com