Privacy and Security in the HITECH Era
Friday, December 16, 2011

FOLEY
FOLEY & LARDNER LLP

Speakers:

Jackie Saue
Partner
Foley & Lardner LLP
Health Care Industry Team

Ken Mortensen
Vice President, Assistant General Counsel & Chief Privacy Officer – CVS Caremark Corporation

Leeann Habte
Associate
Foley & Lardner LLP
Health Care Industry Team

HITECH ACT CMPs

VIOLATION CATEGORY	FOR EACH VIOLATON OCCURING ON OR AFTER FEBRUARY 18, 2009	ANNUAL CAP FOR ALL VIOLATIONS OF AN IDENTICAL PROVISION IN A CALENDAR YEAR
CE did not know (and by exercising reasonable diligence would not have known) that the CE had violated Administrative Simplification provision	$100 - $50,000	$1,500,000
Violation is due to reasonable cause and not to willful neglect	$1,000 - $50,000	$1,500,000
Violation is due to willful neglect and violation is corrected within 30 days, beginning on the first day that the CE knew (or by exercising reasonable diligence would have known) that the violation had occurred	$10,000 - $50,000	$1,500,000
Violation is due to willful neglect and violation is not corrected during such 30-day period	$50,000	$1,500,000

HHS OCR CIVIL ENFORCEMENT

- OCR Civil Enforcement Actions
  - July 2011: **UCLA Health System** was fined $865,500 and entered into a 3 year corrective action plan ("CAP") as a result of unauthorized employees repeatedly looking at the electronic PHI of celebrity and other patients.
  - February 2011: **Massachusetts General Hospital** was fined $1 million and entered into a 3 year CAP due to an employee's loss of documents containing PHI of 192 patients, including those with HIV/AIDS, on a subway train.
  - February 2011: HHS OCR imposes a $4.3 million on **Cignet Health of Prince George's County ("Cignet")** due to Cignet's failure to cooperate with OCR's investigation of the denial of patients' rights to access their medical records.

HHS OCR CIVIL ENFORCEMENT

- OCR Civil Enforcement Actions:
  - December 2010: **Management Services Organization Washington, Inc. ("MSO")** was fined $35,000 and entered into a 2 year CAP based on MSO's disclosure of electronic PHI to an affiliate for marketing purposes.
  - June 2010: **Rite Aid Corporation** was fined $1 million and entered into a 3 year CAP as a result of pharmacies' disposal of prescriptions and labeled pill bottles containing individuals' PHI in industrial trash containers that were accessible to the public.
  - January 2009: HHS OCR/FTC joint investigation of the disposal by **CVS** retail pharmacies of PHI, such as old prescriptions and labels from prescription bottles, in dumpsters that were not secure and could be accessed by the public, resulting in a $2,250,00 fine and a 3 year CAP.
  - July 2008: **Providence Health & Services ("Providence")** was fined $100,000 and entered into a 3 year CAP based on Providence's loss in 2005 and 2006 of electronic backup media and laptop computers containing PHI.

HIPAA CRIMINAL PROSECUTIONS

- Federal Criminal Prosecutions
  - Since 2004, the DOJ has brought 38 criminal prosecutions under HIPAA, 10 of which were brought in 2009, 3 of which were brought in 2010, and 9 of which were brought in 2011.
  - Thirty-two cases resulted in a conviction by plea bargain.
  - One case resulted in a conviction by a jury with a 87 month sentence. *U.S. v. Ferrer* (S.D. Fla. 2006).
  - Remaining cases are either pending or have been dismissed (voluntarily or due to an acquittal).

HIPAA CRIMINAL PROSECUTIONS

- Federal Criminal Prosecutions
  - Majority of cases have been against persons accessing records for purposes of personal gain (e.g., identity theft, submission of false Medicare claims, selling PHI to media).
  - Nine prosecutions were brought against persons alleged to have violated HIPAA without a motive of personal gain.
    - Buyer of medical practice inadvertently disposed of records in a dumpster when moving offices. *U.S. v. Cipolla* (W.D.N.Y. 2011) (voluntarily dismissed).
    - Director of a psychiatric care center reported patient as a serious and imminent public health threat, allegedly knowing that the report was untrue. *U.S. v. Kaye* (E.D. Va. 2011) (acquitted).
    - Clinic employee, who was involved in a dispute with a state agency, accessed the psychiatric records of state employees and wrote a letter to the governor complaining of state employment of persons with psychiatric history. *U.S. v. Apodaca* (D. Ariz. 2010).

HIPAA CRIMINAL PROSECUTIONS

- Prosecutions brought against persons for violations of HIPAA without a motive of personal gain (continued)
  - Physicians and staff at a hospital accessed records of a local TV news anchor out of curiosity. *U.S. Griffin* (E.D. Ark. 2009); *U.S. v. Holland* (E.D. Ark 2009); *U.S. v. Miller* (E.D. Ark. 2009).
  - Employee of UCLA Health System accessed medical records of celebrities and co-workers out of curiosity. *U.S. v. Zhou* (C.D. Cal. 2008).
  - Union president, attending staff meeting, grabbed and refused to relinquish patient medical files. *U.S. v. Marshall* (E.D. Va. 2008) (voluntarily dismissed).
  - Nurse accessed patient's records at the request of a psychologist evaluating the patient's fitness to have custody of a child. Psychologist was not authorized to receive the records under HIPAA. *U.S. v. Junso* (D.S.D. 2006) (sentenced to one year probation and $500 fine).

HHS OCR PILOT AUDIT PROGRAM

- HITECH Act requires HHS to conduct periodic audits of CEs and BAs to ensure HIPAA compliance.
- OCR has announced a pilot program of audits of up to 150 covered entities to assess privacy and security compliance, beginning in November 2011 and concluding by December 2012. (BAs will be included in future audits.)
- OCR will audit as wide a range of types and sizes of CEs as possible.
- OCR will use the audit reports to determine best practices and corrective action, but reserves the right to initiate a compliance review to address a serious compliance issue that arises during the audit.

HHS OCR PILOT AUDIT PROGRAM

- Pilot Audit Program Procedures:
  - CEs selected by OCR for audit will receive a notification letter, requesting documentation within 10 business days.
  - OCR intends to notify CEs between 30 and 90 days prior to an onsite visit.
  - Onsite visits may take between 3 and 10 business days, depending upon the complexity of the organization, and will include interviews of key personnel.
  - After fieldwork is completed, the auditor will provide the CE with a draft final report.
  - The CE will have 10 business days to review and provide written comments back to the auditor.
  - The auditor will complete a final audit report within 30 business days after the CE's response and submit it to OCR.

PPACA AMENDMENTS TO HIPAA STANDARD TRANSACTIONS

- Section 1104 of PPACA required HHS to adopt operating rules for each of the standard transactions, with which CEs would have to comply in addition to complying with the implementation specifications for each such transaction.
- On July 8, 2011, HHS issued an Interim Final Rule, with a compliance date of January 1, 2013. The Interim Final Rule:
  - Amended the definition of "standard transaction" to mean "a transaction that complies with an applicable standard and associated operating rules adopted under this part."
  - Defined "operating rules" to mean "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications as adopted for purposes of this part."
  - Adopted operating rules for eligibility for a health plan transaction and health care claim status transaction.

PPACA AMENDMENTS TO HIPAA STANDARD TRANSACTIONS

- PPACA also contained provisions requiring health plans to certify compliance with the standards and operating rules, and to provide documentation of such compliance, to HHS:
  - By December 31, 2013 for: eligibility for a health plan, health claim status, electronic funds transfers (EFT), and health care payment and remittance advice (ERA);
  - By December 31, 2015 for: health claims or equivalent encounter information, health plan enrollment/disenrollment, health plan premium payment, referral certification and authorization transactions, and health care claims attachments.
- PPACA directed HHS to conduct periodic audits to ensure that health plans (including any entities providing services to health plans pursuant to contract) comply with the standards and operating rules.

PPACA AMENDMENTS TO HIPAA STANDARD TRANSACTIONS

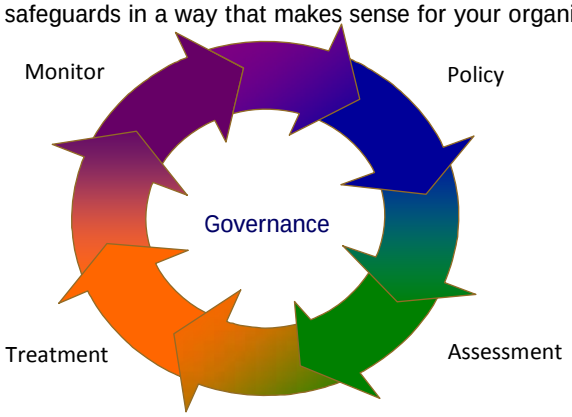
- PPACA Penalties:
  - Not later than April 1, 2014, and annually thereafter, HHS shall assess a penalty against a health plan that fails to meet the certification and documentation requirements in the amount of $1 per covered life for each day that the plan is not compliant, until certification is complete.
  - If the health plan knowingly provides inaccurate or incomplete information in a statement of certification or documentation of compliance, the penalties are doubled.
  - Penalties will be increased on an annual basis by the annual percentage increase in total national health care expenditures, as determined by HHS, subject to certain statutory caps.
  - HHS must establish procedures for assessment of the penalties that provide a health plan with reasonable notice and a dispute resolution procedure prior to a notice of assessment by HHS.

HIPAA Observations

- Many organizations still **do not have a holistic program** to address HIPAA privacy and security requirements
- Early compliance efforts have been focused on creating policies and procedures. However, frequently, there is **a disconnect between policies and actual implementation** of technical and procedural safeguards
- There has been a recent increase of **enforcement** and **audits** of covered entities and business associates

Governance for HIPAA

A sustainable approach to Privacy and Security under HIPAA requires a continuous process that addresses the technical, administrative, and physical safeguards in a way that makes sense for your organization.



Policy

- Top down approach
  - HIPAA should be part of overall privacy and security program
  - Policies best aligned with HIPAA structure
- Lifecycle of information
  - Roles, responsibilities, and authorities
  - Management commitment
  - From creation to destruction

Assessment

- Analysis
  - Risk Assessments
  - Impact Analysis
  - Linking to both HIPAA and business requirements
- Prioritization
  - De-conflict business and compliance needs to optimize risk
  - Define objectives and targets
  - Plan for prevention, deterrence, readiness, mitigation, response, continuity, and recovery

Treatment

- Implementation
  - Determine appropriate controls
    - Privacy: address measures for determining things like, “minimum necessary” and “treatment, payment, health care operations”
    - Security: link control set to appropriate administrative, technical, and physical measures
  - Define the business process
  - Associate with other processes
    - Awareness and training
    - Incident management

Monitor

As solutions are implemented to address identified HIPAA gaps, organizations also need to incorporate HIPAA requirements into business operations as new services and/or systems are introduced into the environment.

Three non-exclusive approaches to monitor compliance associated with HIPAA:

1. **Task Force:** A dedicated team to report on and review new services (or vendors) introduced by lines of businesses from a HIPAA privacy and security standpoint to understand if PHI used or exchanged with customers or third parties and the impact.
2. **Project Management:** Using an IT project discovery process to detect new systems or applications and assess the HIPAA impact and understand if these new applications store or process PHI.
3. **Self Assessment:** Using a periodic HIPAA self-assessment or evaluation process to review the organization's status against HIPAA requirements focusing on high-risk business processes and systems using tools such as the PHI data flow maps.

HITECH Act

- HITECH Act Imposed Additional Requirements on Covered Entities and Other Organizations
  - New breach notification requirements
  - HIPAA privacy and security standards to downstream entities
    - Business Associates (BAs) (including subcontractors)
    - Health Information Organizations, E-Prescribing Gateways, other persons that provide data transmission services
    - Personal Health Record vendors if service provided for Covered Entity (CE)
    - "Workforce members" such as volunteers, trainees, others
  - Further restrictions on uses of PHI
    - Restrictions on marketing and fundraising, prohibitions on sale of PHI added
    - Minimum necessary requirements expanded

HITECH Act (contd.)

- HITECH Act Imposed Additional Requirements on Covered Entities and Other Organizations.
  - Expansion of individual rights
    - Access to and Accounting for Disclosures of PHI in Electronic Health Records (EHRs)
    - Enhancements to Notice of Privacy Practices
    - Health Plan disclosure restrictions.
    - Access to PHI of decedents
  - Increased flexibility for research uses of PHI
    - Compound authorizations
    - Authorizations for future research

Future Compliance Issues

- Omnibus Final Rule Pending (to include breach notification and security, privacy, and enforcement)
  - Proposed Modifications to Privacy, Security, and Enforcement Rules (7/14/10)
  - Breach Notification Interim Final Rule (8/24/09)
  - Enforcement Final Rule (10/29/09)
- Accounting for Disclosures Final Rule Pending
  - Proposed Rule – (5/31/2011)
- Minimum Necessary Rule/Guidance Pending

Breach Notification Program

- Reporting to Congress (8/15/2011)
  - Breaches involving more than 500 Individuals
    - Office for Civil Rights (OCR) received 45 reports in 2009 and 207 reports in 2010.
    - Common causes
      - Theft
      - Loss of electronic media or paper records containing PHI
      - Intentional unauthorized access, use, or disclosure of PHI
      - Human or technological error
      - Improper disposal
  - Breaches of less Than 500 Individuals
    - 5,251 reports in 2009 and 25,000 in 2010
  - Common causes
    - Misdirected communications

Compliance Issues

- Nature of Corrective Actions on Reported Breaches
  - Administrative
    - Revising policies and procedures
    - Training or retraining workforce members who handle PHI
    - Imposing sanctions on workforce members who violated policies and procedures, particularly for serious actions such as removing PHI from the facility against policy, and unauthorized access
    - Performing a new risk assessment
    - Revising Business Associate Agreements (BAAs) to more explicitly require protection for confidential information
  - Physical
    - Improving physical security by installing new security systems or by relocating equipment or records to a more secure area
  - Technical
    - Adopting encryption technologies/changing passwords

Relationships with Business Associates (BAs)

- Pre-HITECH
  - Requirements for BAAs defined in regulation.
  - HIPAA did not directly govern BAs, but required Covered Entities (CEs) to have compliant contracts with BAs.
  - Even if BA was an "agent" of the Covered Entity (CE) pursuant to federal common law, the CE was excepted from liability if (1) the requirements for a BAA were met, (2) the CE did not know of a pattern or practice of the BA violating the agreement, and (3) the CE did not fail to act as required by HIPAA in response to the violation.

Liability for BAs Under HITECH

- Post-HITECH: New Framework for Liability
  - BAs are directly liable for violations of HIPAA and HITECH, even if entities fail to enter into BAA.
    - "Subcontractors" defined as "Business Associates"
    - "Subcontractors" are those persons who perform functions for or provide services to a BA other than in the capacity of a workforce member.
  - Imputes liability to CEs for violation by BAs if "agency" relationship exists
  - Imputes liability to BAs for violations by subcontractors that are "agents"
    - Agency relationship defined under federal common law of agency (fact-specific)
  - Removes express exception to vicarious liability for violations of agent

Requirements for BAs Under HITECH

- Directly Subject to Certain HIPAA Privacy Rules
  - Disclose PHI to HHS for compliance purposes
  - Disclose PHI in electronic format for access to PHI
  - Provide accounting for disclosures in Electronic Health Record (EHR)
  - Comply with minimum necessary standard
  - Take reasonable steps to cure a material breach of subcontractor
- Directly Subject to HIPAA Security Rule
  - Implement administrative, physical, and technical safeguards, and meet policy and documentation requirements

Expanded Requirements for BAAs under HITECH

- Proposed Rule Requires the Following Provisions be Incorporated into BAA
  - Compliance with 45 C.F.R. 164.308, 164.310, 164.312, and 164.316 of the Security Rule with regard to e-PHI
  - Report breaches of unsecured PHI to CEs
  - Ensure that any subcontractors that create or receive PHI on behalf of BA agree to the same restrictions and conditions that apply to BA with respect to such information

Implications for Business Associate Agreements

- Increased Emphasis on Liability Issues
  - Costs and expenses associated with breach notification and mitigation of harm
  - Responsibility for/involvement with risk assessment and breach notification
  - Limits on liability
  - Determination of whether "agency relationship" exists that imputes liability to CE or BA
  - Damages arising from civil actions brought by State Attorneys General for HIPAA violations
  - Costs and expenses associated with investigations of HIPAA violations, criminal conduct, etc.
  - Other damages associated with breach

Compliance

- Ambiguities Regarding Compliance
  - HITECH changes (including requirements for BAs) in Subtitle D generally effective February 1, 2010.
  - Proposed Rule provides for compliance date of 180 days after effective date of Final Rule.
    - Transition provision would grandfather existing BAAs for up to one year beyond the compliance date of the Final Rule, if BAAs not modified between effective date and compliance date of Final Rule.
  - Final Rule still pending.

HIPAA Restrictions on Marketing

- Previous HIPAA Framework for Marketing
  - Authorization required to use or disclose PHI for marketing.
  - Marketing means:
    - A communication about a product or service that encourages recipients of the communication to purchase or use the product or service (with certain exceptions), or
    - An arrangement whereby the Covered Entity discloses PHI to a third party for marketing in exchange for direct or indirect remuneration.
- Marketing Communications Allowed Without Authorization
  - Face-to-face communication
  - Promotional gifts of nominal value to the individual

HIPAA Restrictions on Marketing (contd.)

- Pre-HITECH Did Not Include as Marketing
  - Even if indirect or direct payment from a third party was involved
    - Health care operations communications to describe a health-related product or service that is provided by or included in a plan of benefits of, the CE making the communication, and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits
    - Communications for case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual
    - Communications for the treatment of the individual.

HITECH Revised Framework for Marketing

- Limits Cross-promoting of Products or Services of Other Entities Without Individual's Authorization
  - Certain health care operations communications permitted without authorization, but only if *no financial remuneration* is received in exchange for making communication.
- Permits Individuals to Opt Out of Treatment Communications *if Remuneration is Received* in Exchange for Making the Communication
  - Requires that the Notice of Privacy Practices inform individuals about the remuneration and provide them the right to opt out of receiving further communications
  - The treatment communication must also disclose the remuneration and provide a clear and conspicuous opportunity to opt out of further communications.

HITECH Revised Framework for Marketing (contd.)

- Provides exception to definition of marketing, *even if remuneration is received*, are communications:
  - That only describe a drug or biologic that has been previously prescribed or administered, provided the amount of the remuneration to the supplier is reasonable
- Prohibits Sale of PHI
  - CE or BA may not receive "direct or indirect" financial remuneration in exchange for disclosure of PHI, unless valid authorization provided (with certain specified exceptions).
  - Proposed Rule requires that the individual authorization state that the disclosure will result in financial remuneration to the CE.

Fundraising under HITECH

- Provides Individuals with Right to Opt Out of Fundraising
  - Proposed Rule require that a CE provide, with each fundraising communication, a clear and conspicuous opportunity to opt out of receiving future fundraising communications.
    - No undue burden on individual
    - Cannot condition treatment or payment on an individual's choice
    - May not send such information to individuals who have opted out
  - Must include information about fundraising communications in Notice of Privacy Practices.

More to Come

- Issues That May Be Addressed in Final Rule
  - Modifications to breach reporting
  - Definition of “subcontractor” of Business Associate
  - Amount of payment allowable for communications about drugs , scope of exception to marketing
  - Scope of opt-out for treatment communications and fundraising
  - Exceptions to sale of PHI
  - Whether/how to allow targeted fundraising campaigns by CEs

Question & Answer Session

Speaker Contact Information:

- Jackie Saue, Foley & Lardner – jsaue@foley.com
- Ken Mortensen, CVS Caremark Corporation KPMortensen@cvs.com
- Leeann Habte, Foley & Lardner – lhabte@foley.com

Mark Your Calendars

- There is one remaining session as part of the **Health Information Technology Web Conference Series:**
  - Monday, January 23, 2012 – **Emerging Issues in Health Information Technology**