

HIPAA/HITECH ACT WORKSHOP



CROWE&DUNLEVY
ATTORNEYS AND COUNSELORS AT LAW

Karen S. Rieger

Cori H. Loomis

Agenda

- **9:00-9:45**
- HITECH Amendments
- **9:45-10:00** Break
- **10:00-11:00**
- HIPAA Update and EHR incentives



HITECH Amendments

- American Recovery and Reinvestment Act of 2009 (a/k/a, the Stimulus Bill).
- Title XIII – Health Information Technology for Economic and Clinical Health Act.

HITECH Amendments



- Effective Date –

12 months after enactment, unless otherwise specified.

February 17, 2010.

Top Ten Medical Record Bloopers

10. Patient was alert and unresponsive.
9. Occasional, constant infrequent headaches.
8. The patient is tearful and crying constantly. She also appears to be depressed.
7. The patient has no previous history of suicides.
6. She stated that she had been constipated for most of her life, until she got a divorce.
5. Patient had waffles for breakfast and anorexia for lunch.
4. She is numb from her toes down.
3. Patient has two teenage children, but no other abnormalities.
2. Discharge status: Alive but without permission.
1. The patient refused autopsy.

Business Associates

- HIPAA requirements now directly applicable.
- HITECH security provisions for breach notification also apply.
- Compliance date: February 17, 2010, unless otherwise specified.

Business Associates

- Unclear why business associates agreements continue to be necessary in light of direct regulation.
- Implement and execute strategy for updating agreements.

Breach Notification

- Public notification of data breaches involving 'unsecured' PHI required.
- Covered Entities and Business Associates must comply.



Breach Notification

- Interim guidance by Aug. 18, 2009.
- Released on April 17, 2009.
- Compliance date: Sept. 30, 2009.



Breach Notification

- “Unsecured” PHI
 - PHI not protected by “technologies and methodologies that render PHI unusable, unreadable, or indecipherable.”
 - i.e., not encrypted.

Definition of Secure



- Data must be properly
 - Encrypted or
 - Destroyed.

Definition of Secure

- Standards differ for:
 - Data in motion (e.g., records sent in a wireless transmission),
 - Data at rest (e.g., records stored in a data base); and
 - Data disposed (e.g., discarded paper records or recycled electronic records).

Encryption

- National Institute for Standards and Technology (“NIST”):
 - Encryption of data at rest (Publication 800-11, *Guide to Storage Encryption Technologies for End User*).

Encryption (2)

- Encryption of data in motion (Federal Information Processing Standards (“FIPS”) 140-2, which include the standards set forth in 3 different NIST documents.



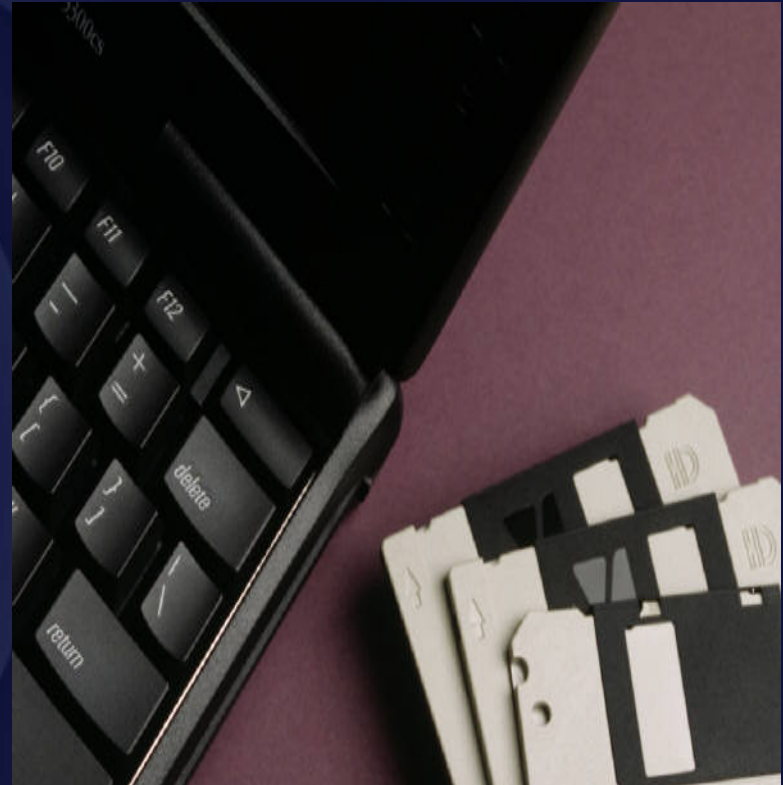
Hard Copy Destruction

- Shredded or destroyed such that it cannot be read or reconstructed.



Electronic Destruction

- Cleared, purged or destroyed in a manner consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation*.



Breach Notification

- Breach deemed discovered on 1st day that breach is known or should reasonably have been known.
- Coordination with business associates a good idea.

Breach Notification

- Individual notice: Within 60 days of discovery.
- Notice to Secretary of HHS:
immediately if breach involves 500 or more people.
 - If less than 500, maintain log and provide log to HHS annually.

Content of Notice

- Brief description of the breach (date of breach and date of discovery);
- Description of the type of PHI involved;
- Steps individuals should take to protect themselves from harm;

Content of Notice (2)

- Steps taken to investigate breach, mitigate loss and prevent future breaches.
- Contact information for affected persons to obtain more information.

Action Plan

- Examine data at rest and data in motion encryption processes, if any.
- Download NIST documents and consider the specified encryption methods with IT managers.

Action Plan (2)

- Explore the costs (both financial and operational) of adopting the specified encryption methodologies and the benefit of avoiding breach notification requirements.

Action Plan (3)

- Examine destruction of PHI methods and policies.
- Download the NIST electronic media destruction policy and analyze and compare against your current policies.

Action Plan (4)

- If unable to ensure that PHI is not “unsecured”, prepare for breach notification obligations.



Minimum Necessary

- Limit requests for, and use or disclosures of, PHI to:
 - A ‘limited data set’ *to the extent practicable*; or
 - *If needed by such entities* to the minimum necessary to accomplish the intended purpose.

Minimum Necessary

- To date, 'limited data set' mainly a concern of entities engaged in research.
- Secretary of HHS will issue additional guidance on minimum necessary requirement by August 17, 2010.

EHR – Expanded Accounting

- Entities using EHRs must provide accounting for all disclosures.
- Formerly, exemption from accounting for disclosures for TPO.

EHR – Expanded Accounting

- Covered Entities must either:
 - Account for disclosures of PHI made by their business associates; or
 - Provide a list of, and contact information for, all business associates acting on behalf of the covered entity.

EHR - Expanded Accounting

- Delayed effective dates
 - EHR Acquired by 1.1.09.
 - Must comply by 1.14.14.
 - EHR acquired after 1.1.09.
 - Must comply by 1.1.11.
 - Secretary may impose later effective dates within limits.

Sale of PHI

- Unless authorized by patient or an exception applies, Covered Entities and Business Associates cannot receive payment for PHI.



Exceptions

- Public health activities;
- Research;
- Treatment;
- A transaction involving the sale of all or part of a covered entity;
- Payment to a business associate for permissible services; and
- Individual copying fees.

Sale of PHI

- Effective only for exchanges that occur 6 months after the Secretary promulgates regulations, which must be drafted by August 17, 2010.

EMR – Access/Disclosure

- If an individual requests, a Covered Entity with an EHR must:
 - Provide copy in electronic format
 - Transmit copy to a designated recipient in an electronic format; and
 - Charge only for labor costs for retrieval.

Fundraising Opt-Out

- Fundraising communications must include clear notification to individuals of their right to opt-out of receipt future fundraising communications.



Disclosure Restriction

- Covered Entities are *required* to accept a restriction on disclosure to a health plan for payment or operation purposes if:
 - The information pertains *only* to a healthcare item or service that the individual has paid for out of pocket in full;
 - Unless the disclosure is otherwise required by law.

Enforcement

- Increased penalties.
- Criminal penalties apply directly to employees, as well as the organization.
- Civil enforcement jurisdiction extended to State attorney generals.

Tiered Civil Penalty Structure

- Apply to any privacy or security violations.
- Apply to covered entities and business associates.
- New tiered-penalty structure based on the level of knowledge of the violation.

Civil Penalties

- Without Knowledge
 - \$100 per violation, not to exceed \$25,000 per calendar year for all violations of an identical requirement.

Civil Penalties

- Reasonable cause and not to willful neglect:
 - \$1,000 per violation, not to exceed \$100,000 per calendar year for all violations of an identical requirement.

Civil Penalties

- Willful neglect and the failure to comply is corrected within 30 days:
 - \$10,000 per violation, not to exceed \$250,000 per calendar year for all violations of the same requirements.

Civil Penalties

- Willful neglect and the violation is not corrected within 30 days:
 - \$50,000 per violation, not to exceed \$1.5 million per calendar year for all violations of an identical requirement.

Criminal Penalties

- Knowing violations: up to \$50,000 in fines and 1 year in prison.
- False pretenses: up to \$100,000, with 5 years in prison.
- Intent to sell: \$250,000 and 10 years in prison.



Implementation Plan

- Review and revise business associate agreements.
- Ensure that PHI is 'not unsecured' or develop a security breach notification process.

Implementation Plan

- Revise policy on using PHI for marketing.
- Revise policy on restrictions of disclosures of PHI.

Implementation Plan

- Revise policy on the 'minimum necessary' standard.
- Revise policy on accounting for disclosures of PHI maintained in electronic health record.

Implementation Plan

- Restrict sale of PHI to comply with new regulation.
- Understand the increased enforcement provisions.

HIPAA Update

- OCR has logged 43,700 privacy complaints since April 14, 2003.
- Resolved 86%.
- 6,000 cases unresolved.

HIPAA Update

- OCR has referred 456 cases to the DOJ and 306 cases to CMS.
- In 2008, 2,210 cases resulted in corrective action.

HIPAA Update

- Top 5 Covered Entities required to take corrective action:
 - Private practices
 - General hospitals
 - Outpatient facilities
 - Health plans
 - Pharmacies

HIPAA Update

- Top 5 Compliance Issues:
 - Improper use and disclosure of PHI
 - Lack of safeguards
 - Lack of patient access
 - Uses and disclosures of more than minimum necessary
 - Lack of or invalid authorization

High Profile Cases

- Britney Spears
 - UCLA Medical Center disciplined employees in 2005 who snooped in Spears' records after the birth of son Preston.
 - Fired at least 13 employees in 2008 for accessing Spears' records when hospitalized for mental health treatment.

High Profile Cases

- George Clooney
 - 27 employees of Palisades Medical Center in North Bergen, NJ were suspended for accessing Clooney's medical records after his motorcycle accident.

High Profile Cases

- “Octomom”
 - California Department of Public Health fined Kaiser Permanente’s Bellflower Hospital \$250,000 for failing to prevent employees from inappropriately accessing medical records of a patient believed to be the mother of octoplets.

Individual Prosecutions

- In medical identity theft cases, prosecutions are often against individuals and not employers.
- Example:
 - In Sept. 06, the Justice Department indicted a former Cleveland Clinic employee for conspiracy to commit health care fraud. Employee stole PHI and sold it for purpose of submitting false medical claims.

Enforcement

- CVS pays \$2.25 million and toughens practices to settle HIPAA privacy case.
 - Improper disposal of PHI such as identifying information on pill bottles.



Other Case Examples

- Routine cases summarized on the Office of Civil Rights website:

www.hhs.gov/ocr/privacy/hipaa/enforcement.

Oklahoma Developments

- Uniform authorization form
- Change to physician-patient privilege, 12 O.S. § 2503.



OCR Guidance

- FAQs about Family Medical History Information: 1.13.09
- FAQs about Disposal of PHI: 2.18.09

Family Medical History

- May a health care provider disclose PHI about an individual to another provider, when such information is requested for the treatment of a family member of the individual?
 - Yes, HIPAA *permits*, but does not *require* such disclosure.
 - Patient may have requested a restriction.

Disposal of PHI

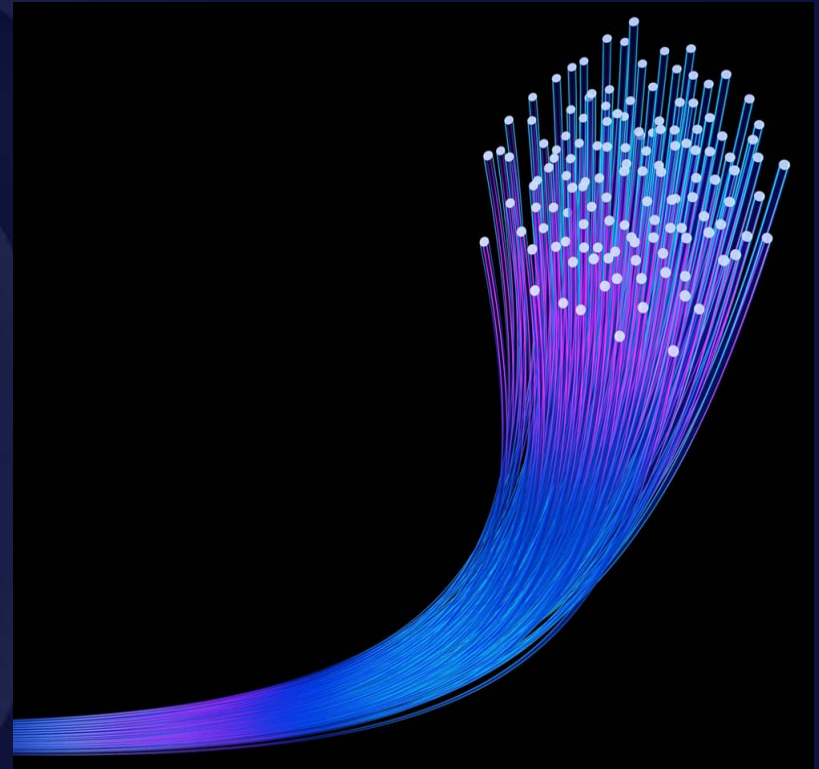
- What do the HIPAA Privacy and Security rules require?
 - Covered entities cannot simply abandon PHI or dispose of it in dumpsters or other containers that are accessible to the public.
 - No particular method is required.
 - May retain BA for disposal services.

Office of National Coordinator

- Released a Privacy and Security Toolkit on 12.15.08
 - Available at:
www.hhs.gov/healthit/privacy/framework.html.
- New guidance documents discuss how the Privacy Rule can facilitate the electronic exchange of health information.

E.H.R. Incentives

- ARRA made \$19 billion available for HIT
- \$17 billion set aside to pay incentives to implement and use HIT



Purposes

- By 2014:
 - Purchase *certified* E.H.R. technology and
 - Use it in a *meaningful way*.

Carrot and Stick Approach

- Payment incentives
- Medicare payment reductions

Qualifications

- Demonstrate:
 - *Meaningful use of*
 - *Certified technology*

DHHS Guidance

- HHS Secretary to adopt standards, implementation specifications and certification criteria no later than December 31, 2009.



Meaningful Use

- Meaningful use of E.H.R. technology:
 - Is determined by the HHS secretary;
 - Includes e-prescribing capabilities;
 - Electronic connection for exchange of health information
 - Utilizes technology to report on clinical quality measures.

Meaningful Use

- Health IT Policy Committee released recommendations on June 16, 2009.
- Recommend a progression wherein *meaningful use* “is ultimately linked to achieving measurable outcomes in patient engagement, care coordination, and population health.”

Measures

- “In identifying potential criteria. . . , it became apparent that there are considerable gaps in E.H.R.-generated measures available to monitor key desired policy outcomes, (e.g., efficiency, patient safety, care coordination).”

Matrix

- Matrix
 - Includes:
 - Outcome priorities,
 - Objectives for 2011, 2013 and 2015;
and
 - Measures for 2011, 2013 and 2015.
- Available at:
<http://healthit.hhs.gov/portal/server.pt>.

Medicaid Incentives

- Each state will define meaningful use of E.H.R. technology for Medicaid incentives.



Incentive Choice

- Providers are only permitted to receive incentives through one program, either Medicare or Medicaid, but not both.

Physician Incentives

- Eligible physicians can receive up to \$44,000 from Medicare over 5 years.
 - 1st year: \$18,000
 - 2nd year: \$12,000
 - 3rd year: \$8,000
 - 4th year: \$4,000
 - 5th year: \$2,000
- Hospital-based physicians are not eligible.

Penalties and Rate Reductions

- Medicare payments reduced by:
 - 1% in 2015
 - 2% in 2016
 - 3% in 2017 and beyond.
- If less than 75% adoption, Secretary can reduce the fee schedule further in 2018.

PPS Hospital Incentives

- If use begins by 2011, eligible for incentives for 4 years.
- Psychiatric, rehab, long-term care, children's and some specialty hospitals are not eligible at this time.

PPS Calculation

- Complex formula consisting of:
 - Base dollar amount;
 - Plus a per discharge amount;
 - Multiplied by the hospital's Medicare share;
 - Times a yearly transition factor.

Medicare Portion

- Involves a combination of:
 - Medicare days (both traditional Part A and Part C),
 - Divided by total inpatient days,
 - Multiplied by the ratio of charges less charity care to total charges.

PPS Hospital Timeline

- 2011-2013: Hospitals may receive 100% of their eligible incentive payment.
- 2013 and after: a transition factor will apply.

Penalties

- First meaningful use after 2015, hospital not eligible for any incentives.
- Phase-out formula for incentives.

Rate Reduction

- Reductions in proposed market basket increases by year:
 - 2015 reduction: 33 1/3%
 - 2016 reduction: 66 2/3%
 - 2017 and each subsequent year reduction: 100%

Getting Prepared

- Don't wait to begin evaluating readiness for E.H.R. technology.
- Infrastructure to support HIT should be in place before 2011.

Implementation Time Frame

- Group of 5 physicians
 - approximately 6 months
- Hospitals
 - a minimum of 18-24 months

Government Goals

- 75% of providers using E.H.R. technology by 2015
- Currently,
 - Fewer than 20% of physicians; and
 - 1.5% of non-federal hospitals.

AKS and Stark Protection

- Final rule became effective Oct. 10, 2006.
- Permits certain donations of technology and related services used in e-prescribing and electronic health records.

AKS and Stark Protection

- Requires:
 - Documentation;
 - Protected technology does not include hardware;
 - Inter-operability;
 - 15% cost sharing for EHR; and
 - Sunsets December 31, 2013.

Issues

- Aggressive timelines and unanswered questions.
- Balance between ensuring timeliness to capitalize on incentives and avoid penalties yet avoiding unnecessary spending associated with lack of guidance.

Questions?

