HIPAA and Public Health: An Update from the HHS Office of Civil Rights

A webinar offered by
The CDC Public Health Law Program
and
The Network for Public Health Law
How To Use Webex

If you can hear us through your computer, you do not need to dial into the call. Just adjust your computer speakers as needed.

If you need technical assistance, call Webex Technical Support at 1-866-863-3904.

All participants are muted. Type a question into the Q & A panel for our panelists to answer. Send your questions in at any time.

This webinar is being recorded. If you arrive late, miss details or would like to share it, we will send you a link to this recording after the session has ended.
HIPAA and Public Health: An Update from the HHS Office of Civil Rights

A webinar offered by
The CDC Public Health Law Program
and
The Network for Public Health Law
Disclaimer

The contents of this presentation are for informational purposes only, have not been formally disseminated by the Centers for Disease Control and Prevention nor the Network for Public Health Law, and should not be construed to represent any agency or organizational determination or policy.
Webinar Co-Sponsors

The Network for Public Health Law

CDC/OSTLT’s Public Health Law Program
CDC/OSTLTS Public Health Law Program

• What we do
  • Advance the use of law as a public health tool

• How we do it
  • Provide technical assistance, publications, legal epidemiology, and workforce development
  • Create tools that can be used to influence public health outcomes

• Whom we serve
  • CDC programs and state, tribal, local, and territorial (STLT) communities
  • You!
The **Network for Public Health Law** provides insightful legal assistance, helpful resources, and opportunities to build connections for local, tribal, state and federal officials; public health practitioners; attorneys; policy-makers; and advocates. The Network serves as a single-entry point to experienced experts on a wide-range of public health law topics.

Attend the **2014 Public Health Law Conference** in Atlanta, GA, October 16 & 17 to learn how law can be used to address critical public health concerns like health reform, emergency preparedness, health information privacy, and chronic disease and injury prevention.

HIPAA and Public Health:
An Update from the HHS Office of Civil Rights

Iliana L. Peters, J.D., LL.M.
February 3, 2014
• Covered Entities and Business Associates
  – Health Plans
  – Health Care Clearinghouses
  – Most Health Care Providers

• Protected Health Information (PHI)
  – Individually Identifiable Health Information
  – Held or Transmitted by Covered Entities or Business Associates
A hybrid entity is a single legal entity:
- That is a covered entity
- Whose business activities include both covered and non-covered functions, and
- That designates its health care components in accordance with the HIPAA Privacy Rule.
Hybrid entities may designate parts of themselves as health care components, and must:

– Comply with the HIPAA Rules.
– Refrain from disclosing PHI inappropriately, including to another component of the hybrid entity.
– May disclose as otherwise allowed if they were separate legal entities.
– Include within-entity business associates in the health care component.
• Covered entities may disclose protected health information to:
  – public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
  – entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance;

[NEXT SLIDE]
• [CONTINUED]
  
  – individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and

  – employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.
• OCR Guidance:  
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/publichealth.html

• CDC Guidance:  
http://www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm
A Reminder of What’s Included:

• Final Modifications of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules pursuant to the Health Information Technology for Economic and Clinical Health Act (the HITECH Act)

• Final Modifications of the Privacy Rule pursuant to the Genetic Information Nondiscrimination Act (GINA)

• Other Modifications to Improve Workability of the Privacy Rule
Changes to the Rules:

• Security Rule: BAs (and subcontractors) now directly liable

• Privacy Rule: BAs (and subcontractors) now directly liable for:
  – impermissible uses and disclosures;
  – non-compliance with their BA Agreements; and
  – certain individual rights.
New Guidance:

The HIPAA Omnibus Rule
https://www.youtube.com/watch?v=mX-QL9PoePU
Changes and New Guidance:

- Authorization required for all treatment and health care operations communications where the CE (or BA) receives financial remuneration for making the communication from a third party whose product or service is being marketed.

- Specific exceptions: face-to-face; promotional gift of nominal value; refill reminders; individual treatment and care coordination.

Changes and New Guidance:

• PHI no longer includes the individually identifiable health information of individuals deceased more than 50 years.

• With respect to family members or other persons involved in the individual’s health care or payment for care prior to the individual’s death, but who are not personal representatives, the Privacy Rule now permits a CE to disclose the relevant PHI of the decedent to such persons, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity.

Changes and New Guidance:

- The Privacy Rule permits a covered provider to disclose proof of immunization about a student or prospective student to a school that is required by State or other law to have such proof prior to admitting the student, if the parent or guardian (or student, if adult or emancipated) agrees.

Must include statements regarding:

- Authorization of use and disclosure of psychotherapy notes;
- Authorization of use and disclosure of PHI for marketing;
- Authorization of sale of PHI;
- Other uses and disclosures not described in the NPP may need Authorization;
- Use and disclosure of PHI for fundraising;
- Right to restrict disclosures to a health plan;
- Right to notification in the case of breach;
- Prohibition on the use of genetic information for underwriting by health plans.
http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
New or Revised Provisions:

• Prohibited Disclosures:
  – Sale
  – Genetic Information for Underwriting Purposes

• Research

• Fundraising

• Right to Request Restrictions

• Access
Revised Definition of “Breach:”

Breach Presumed UNLESS:

• “LoProCo:” The CE or BA can demonstrate that there is a low probability that the PHI has been compromised based on:
  – Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
  – The unauthorized person who used the PHI or to whom the disclosure was made;
  – Whether the PHI was actually acquired or viewed; and
  – The extent to which the risk to the PHI has been mitigated.

Focus on risk to the data, instead of risk of harm to the individual.

Risk Assessment must be documented.
**500+ Breaches by Type of Breach**

- **Unauthorized Access/Disclosure**: 20%
- **Theft**: 50%
- **Loss**: 12%
- **Hacking/IT Incident**: 8%
- **Improper Disposal**: 5%
- **Unknown**: 5%

**United States Department of Health & Human Services**

**Office for Civil Rights**

25
500+ Breaches by Location of Breach

- Paper Records: 22%
- Laptop: 23%
- Desktop Computer: 16%
- Portable Electronic Device: 12%
- Network Server: 12%
- EMR: 3%
- Other: 10%
- E-mail: 2%
September 2009 through October 28, 2013

- 682 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 62% of large breaches
  - Laptops and other portable storage devices account for 35% of large breaches
  - Paper records are 22% of large breaches

- 84,000+ reports of breaches of PHI affecting less than 500 individuals
Appropriate Safeguards Prevent Breaches

• Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives

• Take reasonable and appropriate measures to safeguard e-PHI
  – Store all e-PHI to a network
  – Encrypt data stored on portable/movable devices & media
  – Employ a remote device wipe to remove data when lost or stolen
  – Train workforce members on how to effectively safeguard data and timely report security incidents
• Affinity Health Plan, Inc.: $1,215,780
• WellPoint Inc.: $1.7 million
• Shasta Regional Medical Center: $275,000
• Idaho State University: $400,000
Lessons Learned:

- HIPAA covered entities and their business associates are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect this information.

- Take caution when implementing changes to information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.

- Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients’ rights are fully protected as well as the confidentiality of their health data.
No findings or observations for 13 entities (11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller, Level 4 entities struggle with all three areas
AUDIT PROGRAM NEXT STEPS

Internal analysis for follow up and next steps
- Creation of technical assistance based on results
- Determine where entity follow up is appropriate
- Identify leading practices

Protocol Updates
- Revise CE Protocol to reflect Omnibus Rule
- Develop BA Protocol

Future program design and focus
- Business Associates: Identify the population.
- Identify areas of focus for future audits.
- Accreditation /Certification correlations?
WEDI Summer Webinar Series:

- Introduction to HITECH Changes
- “Dig Deep” into the HIPAA Privacy Rule
- Business Associates
- Breach Notification Rule

http://www.wedi.org/forms/store/CommercePlusFormPublic/search?action=Feature
Medscape Resource Center:

http://www.medscape.org/sites/advances/patients-rights
Medscape Training Videos:

Understanding the Basics of HIPAA Security Risk Analysis and Risk Management
Leon Rodriguez, JD
Director, Office for Civil Rights
US Department of Health and Human Services
Washington, DC


Your Mobile Device and Health Information Privacy and Security
Leon Rodriguez, JD
Director, Office for Civil Rights
US Department of Health and Human Services
Washington, DC
Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
US Department of Health and Human Services
Washington, DC

Consumer Awareness:

**Your New Rights Under HIPAA - Consumers**

https://www.youtube.com/watch?v=3-wV23_E4eQ

Over 262,000 views since September 4, 2013
Mobile Devices:

http://www.healthit.gov/mobiledevices
More Guidance:

- Business Associates
- Breach Notification Rule
- Security Rule
- Individual Rights
- Other Privacy Rule Topics

More Training:

- Online Training Modules
- Audit Program
QUESTIONS?
Thank you for joining us!!

If you have thoughts on topics for future public health law webinars, please email us at: PHLawProgram@cdc.gov
Please join us for this February webinar:

Blocked Shots: Examining the Basis, Nature and Public Health Impact of Vaccine Exemption Laws

Presented by the Network for Public Health Law, Public Health Law Research, and the American Society of Law, Medicine & Ethics

Wednesday, February 19, 2013 at 1 p.m. (ET)

networkforphl.org/webinars