HIPAA and Public Health

Denise Chrysler, JD, The Network for Public Health Law
Joseph A. Guarino, JD, Assistant City Attorney, Kansas City
Alan Holtkamp, JD, Assistant City Attorney, Kansas City

Missouri Public Health Annual Conference, September 22-24, 2015

Workshop outline
1. Overview (20 min)
2. HIPAA (60 min)
3. Break (20 min)
4. Missouri laws (30 min)
5. De-identification (30 min)
6. Wrap-up (20 min)
-- Practice questions & scenarios to apply the law

About the Network for Public Health Law

At no cost, the Network provides public health legal support:

» Technical assistance
» Training and resources
» Opportunities to build connections
» Visit www.networkforphl.org
» Join the Network! (it’s free)

The Fine Print

This presentation is for informational purposes only. It is not intended as a legal position or advice from the presenters or their employers.

For legal advice, attendees should consult with their own counsel.
Overview

Data and Health Information

- Basic to public health practice
- Essential to public health mission
- Foundation for three Public Health Core Functions
- Reflected in ten Essential Health Services
- Must be addressed for Public Health Accreditation

Measure 11.1.3A Policies regarding confidentiality, including applicable HIPAA requirements

Measure 11.1.6A Information management function that supports the health department’s mission and workforce by providing infrastructure for data storage, protection, and management; and data analysis and reporting

Why this workshop?

- Data necessary for local public health to fulfill its responsibilities
- Multiple and conflicting roles and responsibilities
- Amount of electronic data, systems and capabilities growing (connectivity)
- New sources of data
- Employees working remotely
- New communications modes and devices (e.g. social media, smart phones)
- Laws that are confusing and obsolete
- High stakes
Juggling multiple roles and competing interests

- Manage and improve population health AND provider of primary health care
- Protecting individual privacy
- Protecting the public
- Informing the public

Screening
- Childhood lead screening
- Newborn screening for metabolic diseases
- Early hearing detection & intervention
- Vision & hearing screening of school children

WIC

Health Plans
- Medicaid
- State Children’s Health Plan
- County Health Plans

Regulatory
- Restaurant inspection reports
- Septic, wells, other permits
- Clean indoor air act
- Burning ordinances
- Asbestos contractors
- Lead abatement contractors
- Health facilities

Vital Records
- Birth records
- Death records
- Marriage records

Registries
- Cancer
- Birth defects
- Traumatic injuries
- Immunizations

Disease Surveillance
- Infectious disease reports
- Syndromic surveillance
- Hospital acquired infections

Clinical Services
- Child & maternal health
- Immunization
- Dental clinics
- School-based clinics
- FQHCs or CHCs

Emergency Preparedness
- Health alert networks
- Volunteer registries
- Vulnerable people registries
And growing ....
» Amount of data
» Sources of data
» Data sharing partners
» Ways to transfer and exchange
» Linkages with other information
» Creation integrated databases
» Retention, reuse, and further sharing of the information
» Creation of public datasets

So many laws ....

New sources of data

Law governs every aspect of data
Collection Use
Sharing Protection

Law friend or foe?
- How does law help us to do our job?
- How is law a barrier?
Federal laws (examples)
» HIPAA Privacy and Security Regulations
» Family Educational Rights & Privacy Act (FERPA)
» 42 CFR Part 2 (substance abuse)
» Public Health Services Act (Title X family planning)
» Social Security Act (Medicare, Medicaid, SCHIP)
» VA Claims Confidentiality Statute
» WIC Regulations
» National Security Act
» Critical Infrastructure Information Act

State laws (examples)
» Public health laws (e.g., reporting requirements, communicable disease investigations, HIV/AIDS, vital records, registries, confidentiality)
» Health information/medical records laws
» Health information exchange laws
» Identity theft protection; breach notification laws
» Sunshine Law
» Data practices laws

Electronic Data
Benefits & Risks
The stakes are higher …

New challenges from the way we communicate and work:
• Bring your own device
• Working remotely
• Smart phones, tablets, laptops
• Texting
• Instant messaging
• Social media

Health IT.gov
Your Mobile Device and Health Information Privacy and Security
Post Practice question: Social media comments

Emerald City of Oz
Health Department

Your health department wants to provide opportunities for interaction with the community by allowing the public to post comments on its website. But . . . you are concerned that individuals might post comments that are contrary to the public health message, e.g., anti-vaccine comments that are not based on science.

Q: Can your health department “control the message” by deleting comments that undermine public health’s mission?

Risk of liability

» Lawsuits
- Andrew Speaker sued CDC and claimed that CDC had breached his privacy by revealing his name to the press
- Missouri recognizes a cause of action for invasion of privacy when there has been an infringement of the right to not have a public disclosure of private facts. Sullivan v. Pulitzer Broadcasting Co., 709 S.W.2d 475 (Mo. 1986)

Risk of liability (HIPAA)

» Complaints & audits
» Civil fines
- Alaska Dept of Health & Social Services settles HIPAA security case for $1.7 million (electronic Medicaid info)
- Skagit County, WA settles HIPAA case for $215,000; county public health department
Skagit County (population 118,000)

“This case marks the first settlement with a county government and sends a strong message about the importance of HIPAA compliance to local and county governments, regardless of size,” said Susan McAndrew, deputy director of health information privacy at the HHS Office for Civil Rights (OCR). “These agencies need to adopt a meaningful compliance program to ensure the privacy and security of patients’ information.”

Ultimate risk:
losing community trust

- Residents
- Partners and stakeholders
- Ammunition for opponents of government’s authority to obtain information about individuals without consent

Practice question
(submitted by a Missouri public health practitioner)

» To create a meaningful compliance program, is it necessary for my health department to expend thousands of dollars on consultants, software, and training?

Meaningful compliance

» Appoint privacy and security officers
» Determine HIPAA applicability; identify other laws that apply
» Develop policies, procedures, protocols
» Train your employees
» Conduct a risk assessment (electronic info)
» Monitor compliance, take action re noncompliance
» Document, retain records
» Fact sheets, tools, training materials available free of charge (see Resources list)
HIPAA Regulations

What is HIPAA?
Health Insurance Portability & Accountability Act

It’s more than privacy . . .
- Electronic transactions
- Privacy
- Security
- Breach notification

What does HIPAA do? (privacy)
- Requires appropriate safeguards to protect the privacy of personal health information
- Sets limits and conditions on uses and disclosures that may be made of such information without patient authorization
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections

HIPAA basics
- What is it?
- What does it do?
- What does it cover?
- To whom does it apply?
- What does it require?
- What does it allow?
- What is a breach?
- What must be done?
- How is it enforced
- What are the penalties?
What does HIPAA do? (security)

» Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI (ePHI)

» ePHI = transmitted by electronic media or maintained in electronic form

What does HIPAA do?

» Includes provisions regarding compliance, and investigations, imposition of civil money penalties for violations of HIPAA and procedures for hearing

To whom does HIPAA apply?

» Certain health care providers

» Health plans

» Health care clearinghouses

» Called “covered entities”

» OCR “Am I a covered entity?” tool

» Business Associates of a covered entity

Certain health care providers

» Broad definition includes doctors, clinics, psychologists, dentists, nurses, pharmacies, etc.

» But only if they transmit information in electronic form in connection with an electronic standard transaction that HHS has adopted a standard

- Basically means that provider has to communicate electronically with health plans/payors

- E.g. request for payment, eligibility check, prior authorization, etc.
Health plans
» Health insurance companies
» HMOs
» Company health plans
» Government programs that pay for health care
e.g. Medicare, Medicaid, SCIP
» But does not include government grants to fund health care

Must train all workforce members on privacy policies, procedures and what is necessary and appropriate for them to carry out their duties
» Workforce – Employees, volunteers, trainees, and other persons whose conduct in under your direct control

Does HIPAA apply to:
» All of my health department?
» Some of my health department?
» None of my health department?

Hybrid entity means a single legal entity:
» That is a covered entity
» Whose business activities include both covered and non-covered functions; and
» That designates health care components by separating them from its other components and documenting the designation
**Is your governmental entity a hybrid? Should it be?**

**Pros:**
- Reduce compliance costs
- Avoid HIPAA challenges when implementing non-health programs
- Reduce exposure to liability

**Cons:**
- Must follow procedures to create a hybrid
- Apply different privacy standards depending on program
- Administrative and technical requirements

**Practice questions – does HIPAA apply to:**

- Vision screening program?
- Title X family planning grants?
- Immunization clinic?

**Business Associates**

- A person or organization that is not a member of CE's workforce
- Performs functions on behalf of CE or provides services to CE
  - Where access to PHI is involved
  - Examples: billing services; document destruction services; outside attorneys and accountants; computer service technicians; software vendors; cloud computing vendors
- Must have written agreement (BAA)

**Practice questions**

- Missouri law requires Community Hospital to report PHI regarding communicable diseases, cancer, birth defects, etc. Because it provides you with PHI, Community Hospital sends you a BAA. Should you sign and return this BAA?
- Your university asks you to provide field placements for its MPH students. As part of these placements, students will have access to PHI. Should your health dept require that the university sign a BAA?
What does HIPAA cover?

**HIPAA Privacy Rule covers**

- **Use and disclosure of protected health information (PHI)**
  - Use – The sharing, employment, application, utilization, examination, or analysis of PHI within the entity that maintains the PHI
  - Disclose – The release, transfer, provision of access to, or divulging in any manner of PHI outside the entity holding the PHI

**Protected health information (PHI)**

- Information, including demographic information:
  - In any form: written, electronic or oral
  - Relating to past, present or future
  - Physical or mental health status or condition
  - Provision of health care
  - Payment for provision of health care
- That identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual
- No longer PHI 50 years after individual’s death

**What does HIPAA cover?**

**PHI does not include:**

- Education records (FERPA)
- Research records help by non-covered entities
- Employment records that may contain health information
- Health information health by governmental entities that are not covered entities
- De-identified information (see PHI reference card)

More to come – de-identifying information

**Is aggregate data PHI?**

<table>
<thead>
<tr>
<th>2009 pediatric H1N1 cases by county</th>
<th>&lt; 1year</th>
<th>1-5years</th>
<th>6-10yrs</th>
<th>11-17yrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auburn</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Beacon</td>
<td>10</td>
<td>18</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Calhoun</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Davis</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Eaton</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Fulton</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
What does HIPAA require? Privacy:
Basic rules
» Covered entities are prohibited from using or disclosing PHI unless required or allowed by HIPAA privacy rule
» Rule provides numerous exceptions that permit disclosure
» If another law provides greater privacy protection or greater rights to individual concerning his/her health information, must comply with the other law

Minimum necessary rule
» Except for treatment purposes, must limit uses and disclosures of PHI to the minimum amount necessary to accomplish the intended purpose
  - Do not disclose more information than required
  - Do not access information you don’t need

What does HIPAA allow?
Major exceptions to privacy prohibition
» To patient (or legal representative, e.g. generally parent access to child’s info)
» TPO
  - Treatment: provision, coordination, management of care/related services including consults and referrals
  - Payment for health care – reimbursement for health care, coverage, all related activities
  - Health care operations – next slide

Exception – health care operations
» Activities directly related to treatment and payment
  (e.g. utilization review, quality assessment, training)
» Supporting activities
  (e.g. computer systems support, in-house legal counsel)
» Administrative and managerial activities
  (e.g. business planning, resolving complaints, complying with HIPAA)
Exception – Family & Friends
» May disclose PHI to family, relatives, friends involved in individual’s care / payment for care
» If individual present, opportunity to agree or disagree to disclosure (can be inferred)
» Can use professional judgment
» Give individuals ability to designate someone / revoke designation
- See OCR guidance on “family & friends”
» Generally, personal representative can exercise all right of individuals

Practice question: Parent’s right to obtain health care records of child vs. minors’ privacy rights
» Does a parent have the right to obtain his or her child’s health information?
  For family planning services?
  For STD diagnosis and treatment?
  For prenatal care?
  For 17 year old who is married?
  For HPV vaccine?

Practice question (Submitted by a Missouri public health practitioner)
» Our client is back for an appointment. A family member or friend asks how long the client will be. Or, the family member or friend may be providing a ride for the client and wants to know if the client has left.
» Our staff tells them that they can’t confirm that the person is in the building. Then, the family member or friend becomes angry at staff.
Is there anything we can do to address this problem?

Public health in population health role
» Health care providers are crucial source of PHI needed by health departments to protect and improve the public’s health
» Most health care providers are covered by HIPAA
» Providers may question or deny access to information
Practice question
(Scenario is based on problem raised by Missouri public health practitioner)
» Community Hospital notified your health department that one of its employees has been diagnosed Hepatitis C. The employee has been providing patient care for the last two years. The hospital provides you with a list of names and contact information for patients whomight have been exposed. However, the hospital refuses to provide access to patient medical records and to employee-related records, citing HIPAA.
» How do you respond?

MO Public Health Conference, 09/22/2015

Collection & use of data
» Public health broad authority to collect data to prevent and control disease and protect public health (1977 S. Ct opinion, Whalen v Roe)
» Established by state law
» Corresponding duty to protect information
» HIPAA should not impede public health data collection functions
» See resource: HIPAA Privacy Rule and Public Health, Guidance from CDC and HHS

MO Public Health Conference, 09/22/2015

Practice question
(from a Missouri public health practitioner)
» Front desk has had cases where they can’t receive immunization records without a release. As we understand it, immunization records are exempt, but that doesn’t work sometimes. It hinders our job duties. Having clarification in the HIPAA exemptions would be useful and what to do when an outside clinic insists that we need releases to receive necessary information.

MO Public Health Conference, 09/22/2015

HIPAA exceptions that allow disclosure to public health departments
» “Required by law” – mandate contained in law that is enforceable in a court of law
  - Law includes statutes, administrative rules, executive orders (such as under Emergency Management Law), court-ordered subpoenas, etc.
» “Public health” – to public health authorities and their authorized agents for public health purposes, including but not limited to public health surveillance, investigations, and interventions

MO Public Health Conference, 09/22/2015