The Network for Public Health Law

Ideas. Experience. Practical answers.

HIPAA Facts & Fiction

Missouri Center for Public Health Excellence
February 6, 2024

Moderator
Colleen Healy Boufides, Co-Director, Mid States Region, Network for Public Health Law
Presenter
Meghan Mead, Senior Attorney, Mid States Region, Network for Public Health Law

The Network for Public Health 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)**

Objective

To equip public health practitioners with HIPAA basics, terminology, and strategies to maximize access to and the exchange of public health information while maintaining the public's trust

The Network for Public Health Law

Agenda

1. HIPAA Presentation (100 minutes including a 10 minute break)
   - Basics
   - Permissible disclosures (privacy)
   - Security rule
   - Breaches, enforcement, and compliance
   - De-identification of PHI
   - Missouri law
2. Sharing out – what are the HIPAA issues that you have or are currently facing (10 minutes)
3. Q&A (10 minutes)

The Network for Public Health Law

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 employer.

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

The Network for Public Health Law

The Network for Public Health Law
Privacy Officer Peer Group

Join the Local Privacy Officer Peer Group

- Support, resources, and learning opportunities
- Quarterly webinars
- Directory of privacy officers in local public health
- Listserv to connect directly
- No cost

Save the Date for 2024 local privacy officer peer group webinar on March 13 3 p.m. ET/2 p.m. CT

Sign Up https://www.surveymonkey.com/r/6XKB8S7

Contact Stephen Murphy smurphy@networkforphl.org




The Network for Public Health Law

HIPAA Basics

Covered entities and hybrids, business associates, PHI, minimum necessary and more!

The Network for Public Health Law

What does HIPAA do? (privacy)

- **Requires appropriate safeguards to protect the privacy of protected health information**
- **Sets limits and conditions on uses and disclosures without patient authorization**

What does HIPAA do? (privacy)

» **Gives patients rights over their health information**

- Right to access
- Right to request amendment of PHI
- Right to request confidential communications
- Right to an accounting of disclosures
- Notice of privacy practices

What does HIPAA do? (security)

- Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI
- ePHI = transmitted by electronic media or maintained in electronic form

What does HIPAA do? (enforcement)

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

HIPAA applies to most health care providers.

True

False

The Network for Public Health Law

HIPAA applies to most health care providers.

✓ True

To whom does HIPAA apply?

» **"Covered entities" ("CE")**

- Certain (most) health care providers
- Health plans (including government health plans)
- Health care clearinghouses

» **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**

- Essentially means that it only applies where the provider is communicating electronically with health plans/payors
- E.g. request for payment, eligibility check, prior authorization, etc.

The Network for Public Health Law

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**

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 business associate agreement (BAA)**

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; or
  - 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**

PHI does not include:

- No longer PHI 50 years after individual's death
- Student records
- Research records held by non-covered entities
- Employment records that may contain health information
- Health information held by governmental entities that are not covered entities
- De-identified information

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

The Network for Public Health Law

All public health departments are required to comply with HIPAA.

True

False

The Network for Public Health Law

All public health departments are required to comply with HIPAA.

✗ False

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 department 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

The Network for Public Health Law

My health department (or program) is not covered by HIPAA. This means that I don't need to know what HIPAA says.

True **False**

The Network for Public Health Law

My health department (or program) is not covered by HIPAA. This means that I don't need to know what HIPAA says.

ⓧ False

Public health in population health role

- Health care providers are crucial source of health information needed to protect and improve the public's health
- Most health care providers are covered by HIPAA
- Providers may question or deny access to information

The Network for Public Health Law

HIPAA covers all health information.

True

False

HIPAA covers all health information.

✗ False

Aggregate data does not identify individuals. This means that I can release the data below with no HIPAA concerns.

2023 pediatric measles cases by county

	< 1year	1-5years	6-10yrs	11-17yrs
A	2	0	1	3
B	10	18	7	6
C	0	4	1	2
D	4	1	2	1

True

False

Aggregate data does not identify individuals. This means that I can release the data below with no HIPAA concerns.

2023 pediatric measles cases by county

	< 1year	1-5years	6-10yrs	11-17yrs
A	2	0	1	3
B	10	18	7	6
C	0	4	1	2
D	4	1	2	1

✗ False

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**

Permissible disclosures

Basic Rule: Covered entities are prohibited from using or disclosing PHI unless required or allowed by HIPAA privacy rule

HIPAA Privacy Requirements

- 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. 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 rights of individual**

Additional Exceptions

- As required by law
- Abuse, neglect, or intimate partner violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Research

The Network for Public Health Law

A local health department runs an STI testing and treatment clinic. A patient enters the clinic room accompanied by two friends. Under HIPAA, clinic staff may not discuss the patient's test results in front of the friends.

True

False

The Network for Public Health Law

It is reasonable for the provider to infer that if the patient brought their friends to the clinic and into the room with them, the patient has consented to the disclosure of PHI.

Ⓧ False

Public Health: Collection & use of data

- **Public health has 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**

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**

The Network for Public Health Law

HIPAA prohibits Community Hospital from reporting a case of Hepatitis C to my health department, absent the patient's authorization.

True

False

The Network for Public Health Law

HIPAA prohibits Community Hospital from reporting a case of Hepatitis C to my health department, absent the patient's authorization.

✗ False

Minimum necessary rule

» **Minimum necessary applies to disclosure to public health officials for public health purposes**

» **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

The Network for Public Health Law

A health department is investigating an outbreak of Hepatitis C at Community Hospital. It is entitled to look at all of Community Hospital's patient records.

True

False

The Network for Public Health Law

A health department is investigating an outbreak of Hepatitis C at Community Hospital. It is entitled to look at all of Community Hospital's patient records.

✗ False

The Network for Public Health Law

Community Hospital should determine what records are necessary for my investigation, and provide these to me as the "minimum necessary."

True **False**

The Network for Public Health Law

Community Hospital should determine what records are necessary for my investigation, and provide these to me as the "minimum necessary."

✗ False

Healthcare IT News

Published on *Healthcare IT News* (http://www.healthcareitnews.com)

Judge rules hospital must provide EMR access in hepatitis C case

By *Erin McCann, Associate Editor*
Created *11/02/2012*

New Hampshire's Merrimack County Superior Court issued an order Thursday requiring Exeter Hospital to provide access to its electronic medical record database, so public health officials can continue their investigation into a major hepatitis C outbreak.

When a health care provider refuses to provide access (without an authorization)

- Statements of authority (laws that mandate data sharing)
- Explain that HIPAA still permits public health authority to access needed information
- Covered entity may rely on government's written statement regarding its authority, or if written statement impracticable, on oral statement of such authority

HIPAA Resources

» **Public health exception to HIPAA explained:**

- "HIPAA Privacy Rule and Public Health, Guidance from CDC and the U.S. Department of Health and Human Services" http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

HIPAA and immunization records

» **Treatment (other providers, PH immunization clinic)**

» **Public Health (immun clinic, IIS, health dept to school)**

» **Health care provider/CE may disclose to a school, about an individual who is a student or prospective student of the school:**

- Limited to proof of immunization
- Law must require proof of immunization to attend school
- Covered entity obtains and documents agreement to the disclosure (may be oral)

HIPAA and public health emergency preparedness and response

- As required by law
- To public health authority
- To identify, locate, and notify family members
- To disaster relief agency
- To avert a serious and imminent threat to health and safety of a person or the public
- To protect national security
- To law enforcement under certain circumstances
- For judicial or administrative proceedings

The Network for Public Health Law

State law requires Community Hospital to report PHI regarding communicable diseases, cancer, and birth defects to the state health department. Because it provides you with PHI, Community Hospital sends you, the contact at the state health department, a business associate agreement (BAA) to sign and return to them. Should you sign and return this BAA?

True **False**

The Network for Public Health Law

State law requires Community Hospital to report PHI regarding communicable diseases, cancer, and birth defects to the state health department. Because it provides you with PHI, Community Hospital sends you, the contact at the state health department, a business associate agreement (BAA) to sign and return to them. Should you sign and return this BAA?

✗ False

The Network for Public Health Law

A hospital discloses to the local public health authority that a patient contracted a communicable disease but does not provide any additional identifiable information about the patient. This is correct because HIPAA does not permit covered entities to share identifiable information with public health authorities.

True **False**

The Network for Public Health Law

A hospital discloses to the local public health authority that a patient contracted a communicable disease but does not provide any additional identifiable information about the patient. This is correct because HIPAA does not permit covered entities to share identifiable information with public health authorities.

The Network for Public Health Law

HIPAA's Security Rule

Security challenges with the way we communicate and work:

- Bring your own device
- Working remotely
- Smart phones, tablets, laptops
- Texting
- Instant messaging
- Social media

Key Takeaways – Security Rule

» **National standards for protecting PHI held or transferred in electronic form**

» **Flexible and scalable**

» **Risk analysis and management**

» **Implement safeguards - Required vs. addressable**

- Administrative
- Physical
- Technical – Access, Audit, Integrity, Transmission

- **A public health agency operates a mobile immunization and family planning clinic, making it a covered entity. Only a small portion of its workforce provides patient services. What are some of the security considerations here?**

The Network for Public Health Law

HIPAA's Breach Rule & Enforcement

What is a breach?

- **Impermissible use or disclosure that compromises the security or privacy of PHI**
- **Breach presumed *unless* can demonstrate low probability that PHI has been compromised**
- **Risk assessment – four factors**

What must be done?
Breach notification laws

- **HIPAA – notify**
  - Patient
  - Secretary of HHS (all security incidents reported yearly; breaches over 500 reported individually)
  - Media (breach over 500 people)
- **Determine whether your state has a breach notification law**

How is HIPAA enforced?

- **Complaints, investigations, audits**
- **Federal enforcement**
- **HIPAA does not provide a private cause of action . . . but, an individual may still have a claim under state law for a breach of confidentiality or invasion of privacy**

What are the penalties?

- **Civil money penalties – based on nature and extent of violation and harm resulting from violation**
- **Criminal – HHS Office for Civil Rights can refer complaint to Department of Justice**

The Network for Public Health Law

Public health departments have been fined for HIPAA violations.

True

False

The Network for Public Health Law

Public health departments have been fined for HIPAA violations.

✓ True

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

Meaningful compliance (partial list)

- **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 regarding noncompliance**
- **Document, retain records**

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**

Resources, tools

» See Network handout with links to numerous resources and tools.

The Network for Public Health Law

De-Identification

can be a key to open doors

De-Identification under HIPAA

» **Two methods:**

(1) Expert Determination

(2) Safe Harbor

» **See, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule on handout.**

De-Identification – Expert Determination

- Person with appropriate knowledge and experience
- Applies statistical or scientific principles
- Determines very small risk that anticipated recipient could identify individual
- May use mitigation strategies to reduce risk
- Documents methods and results of analysis

De-Identification – Safe Harbor

- HIPAA lists 18 identifiers that must be removed
- Of the individual and of relatives, employers, or household members of the individual
- Very small risk that anticipated recipient could identify individual

The Network for Public Health Law

Missouri State Law

Missouri Public Health Data Collection and Reporting

- Communicable and other specified diseases to local health authority or state department (19 CSR 20-20.020)
- Hospitals, surgical centers, or other healthcare facilities must report hospital acquired infections.
- Health care providers must report charge data, patient abstract data, and financial information.
- Cancer registry; brain and spinal cord injuries
- Department must also compile and issue reports on vital statistics and disease
- Department must also have access to infection rates and treatment at hospitals, et al.

Missouri Privacy and Confidentiality

- Reportable disease information reported under communicable disease rule
- HIV status and test results
- Genetic information
- Mental health records (professionals)
- Mental health and substance use treatment (facilities)
- Immunization records

Missouri Breach Reporting

- Missouri has its own breach reporting law
- Notify consumers in event of a breach.
  - Includes medical or health insurance information
- No private right of action
  - Attorney General has exclusive enforcement authority

Missouri Right to Privacy

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)

The Network for Public Health Law

Q&A and HIPAA issues

What are your HIPAA experiences?

- Share your experience!
- How has HIPAA intersected with your public health practice and what can we learn from you?
- Are you facing a current (or on-going) HIPAA issue and can we help?

➢ **OR**

- General questions on HIPAA?
- Questions on the presentation?

The Network for Public Health Law

Thank you! Please reach out with any questions mmead@networkforphl.org.

And please join us for the next training, Public Health Law 201, on March 6 @ 10am.