How to Use Webex Q & A

1. Open the Q&A panel
2. Select “All Panelists”
3. Type your question
4. Click “Send”
Presenter

Jennifer Bernstein, J.D., Deputy Director, The Network for Public Health Law Mid-States Region

- J.D., M.P.H., University of Iowa
- Research interests/areas of expertise:
  - HIPAA
  - Health Equity
  - Health Information and data sharing
  - Mental Health and Trauma informed care
  - Sexual, reproductive and maternal health
Objective

Equip public health practitioners with HIPAA basics, terminology, mythbusters, and strategies to maximize access to and the exchange of health information while maintaining the public’s trust.
HIPAA basics

» What is it?
» What does it do?
» To whom does it apply?
» What does it cover?
» What does it require?
» What does it allow?
» What is a breach?
» What must be done?
» How is it enforced
» What are the penalties?
“HIPPA” stands for the “Health Information Privacy Protection Act.”

True False
“HIPPA” stands for the “Health Information Privacy Protection Act.”

False
What is HIPAA?

Health Insurance Portability & Accountability Act

It’s more than privacy . . .

» Electronic transactions
» Privacy
» Security
» Breach notification
Data protection =

- Applies to health information in all forms
- Defines circumstances in which identifiable information may be used and disclosed

- Applies to health information in electronic form
- Requires safeguards to protect data from unauthorized access

Images: http://blog.eiqnetworks.com/
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
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 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
HIPAA applies to most health care providers.

True  False
HIPAA applies to most health care providers.
To whom does HIPAA apply?

» Certain (most) health care providers
» Health plans
» Health care clearinghouses
» Called “covered entities” (“CE”)
» 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
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)
All public health departments are required to comply with HIPAA.

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

True
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 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
HIPAA covers all health information.
HIPAA covers all health information.

❌ False
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:

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

2009 pediatric H1N1 cases by county

<table>
<thead>
<tr>
<th>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>
</tbody>
</table>
Aggregate data does not identify individuals. This means that I can release the data below with no HIPAA concerns.

### 2009 pediatric H1N1 cases by county

<table>
<thead>
<tr>
<th>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>
</tbody>
</table>

xic False
Is aggregate data PHI?

2009 pediatric H1N1 cases by county

<table>
<thead>
<tr>
<th>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>
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
HIPAA prohibits my local school district from providing to my local health department routine vaccination information about individual students, absent the parent’s consent.
HIPAA prohibits my local school district from providing to my local health department routine vaccination information about individual students, absent the parent’s consent.

False
What does HIPAA cover?

PHI does not include education records that are covered by the Family Educational Rights Privacy Act (FERPA)

Records that are

- Directly related to a student; and
- Maintained by a school or a party acting for the school, (includes a nurse employee and a nurse contractor)

» Includes transcripts, disciplinary records, and similar records.

» Includes immunization and other medical or health related records
Pleasant Valley School has a measles outbreak. HIPAA prohibits the school from sharing information with our local health department that identifies students who have not been vaccinated against measles.
Pleasant Valley School has a measles outbreak. HIPAA prohibits the school from sharing information with our local health department that identifies students who have not been vaccinated against measles.
HIPAA vs. FERPA

» **HIPAA Privacy Rule** – applies to:
  - Health plans and health care providers that transmit information electronically regarding covered transactions (related to payment for health care)
  - “Protected health information” – individually identifiable information related to patient health status, condition, care, or payment

» **Protected health information**
  - Excludes individually identifiable health information in education records covered by FERPA

» **Bottom line**: If FERPA applies, HIPAA does not
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
Permissible disclosures

Basic Rule: Covered entities are prohibited from using or disclosing PHI unless required or allowed by HIPAA privacy rule.
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
HIPAA prohibits Community Hospital from reporting a case of Hepatitis C to my health department, absent the patient’s authorization.
HIPAA prohibits Community Hospital from reporting a case of Hepatitis C to my health department, absent the patient’s authorization.
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
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
I am investigating an outbreak of Hepatitis C at Community Hospital. I am entitled to look at all of Community Hospital’s patient records.

True False
I am investigating an outbreak of Hepatitis C at Community Hospital. I am entitled to look at all of Community Hospital’s patient records.

False
Minimum necessary applies to disclosure to public health 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
Community Hospital should determine what records are necessary for my investigation, and provide these to me as the “minimum necessary.”

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

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

- **Statements of authority**
- **HIPAA does not impact public health’s authority**
- **Covered entity may rely on government’s written statement regarding its authority, or if written statement impracticable, on oral statement of such authority**
HIPAA and immunization records

» Treatment (other providers, PH immun 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
Public health departments have been fined for HIPAA violations.

True
Public health departments have been fined for HIPAA violations.
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
Risk of liability

» Lawsuits
- Breach of privacy lawsuits
- Andrew Speaker sued CDC and claimed that CDC had breached his privacy by revealing his name to the press

» State civil and criminal penalties
- Public health employee who knowingly releases confidential information is guilty of a misdemeanor
Ultimate risk: losing community trust

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

Impermissible use or disclosure that compromises the security or privacy of PHI
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
HIPAA Breach Notification Safe Harbor

» Don’t have to notify if:

- PHI was encrypted, or
- PHI was disposed consistent with HHS guidance on secure disposal
How is HIPAA enforced?

» Complaints, investigations, audits
» Federal enforcement
» State 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 (see next slide)
- Criminal – HHS Office for Civil Rights can refer complaint to Department of Justice
# Civil penalties for HIPAA Violations

<table>
<thead>
<tr>
<th>Culpability for violation</th>
<th>Per violation</th>
<th>Maximum for identical violation of same HIPAA provision per calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1,000 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect – corrected in timely manner</td>
<td>$10,000 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect – not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Contact

Jennifer Bernstein, J.D., Deputy Director, The Network for Public Health Law Mid-States Region

- Phone: 734-764-6772
- Email: jbernstein@networkforphl.org
How to Use Webex Q & A

1. Open the Q&A panel
2. Select “All Panelists”
3. Type your question
4. Click “Send”
Thank you for attending

For a recording of this webinar and information about future webinars, please visit networkforphl.org/webinars

You may qualify for CLE credit. All webinar attendees will receive an email from ASLME, an approved provider of continuing legal education credits, with information on applying for CLE credit for this webinar.