Human Subjects Research & the HIPAA Privacy Rule
Overview

• HIPAA & Research
• Increased Enforcement
• Data Security
HIPAA & Research
What is HIPAA?

**Health Insurance Portability and Accountability Act** - what is it?

**Privacy rule**
- Disclosure of protected health information (PHI) is strictly regulated
- Covered entities, hybrid entities, business associates
Protected Health Information

Information about health status, provision of care, or payment for care created or collected for a covered entity (paper and electronic formats)

(1) Names (including initials);
(2) Street address, city, county, precinct, zip code, and equivalent geo-codes
(3) ALL elements of dates (except year) for dates directly related to an individual and all ages over 89 (this would include procedure dates, date of admission, date of lab work, etc.)
(4) Telephone numbers;
(5) Fax numbers;
(6) Electronic mail addresses;
(7) Social security numbers;
(8) Medical record numbers;
(9) Health plan ID numbers;
(10) Account numbers;
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers/serial numbers;
(14) Web addresses (URLs);
(15) Internet IP addresses;
(16) Biometric identifiers, incl. finger and voice prints;
(17) Full face photographic images and any comparable images; and
(18) Any other unique identifying number, characteristic, or code
Do you work with Protected Health Information?

Do you work in a Covered Health Care Component?
- Dentistry
- Health System
- Nisonger
- Optometry

Do you work with data from a Covered Health Care Component?
- Business associates: Medicine, Nursing, Pharmacy
- MOUs for research: Public Health, Engineering
- Colleagues outside OSU
Reminder

Even if HIPAA is not a concern for your research, human research regulations may still apply – along with the need to protect the confidentiality of subjects and the data
HIPAA & Research

HIPAA & Research

**PHI Use for Research**
- Patient Authorization
- Full Waiver
- Partial Waiver
- Preparatory to Research
- Decedents
- Limited Data Sets

**PHI Disclosure for Research**
- Patient Authorization
- Full Waiver
- Partial Waiver
- Preparatory to Research
- Decedents
- Limited Data Sets

Minimum Necessary
Research Requirements

HIPAA Authorization
• Specific elements
• Signed by patient or personal representative
• Retain for 6 years

Waiver of HIPAA Authorization
• Factors to consider
• Retain for 6 years
HIPAA Research Authorization Elements

Core Elements
• Description of PHI to be used or disclosed
• Names of those authorized to make requested use/disclosure
• Names of those who may use the PHI or to whom the elements may make the requested disclosure
• Description of each purpose
• Expiration date of authorization
• Signature and date

Required Statement
• Individual’s right to revoke
• Notice of CE’s ability or inability to condition treatment, payment, enrollment, eligibility for benefits on the authorization
• Potential for redisclosure by the recipient and no longer protected by Privacy Rule

HIPAA Research Authorization Form

• Combined with consent document
  • “Compound authorization”
• Stand-alone
Exceptions

- De-identified data
- PHI of deceased
- Limited Data Set
- Preparatory to research
“Regardless of the method by which de-identification is achieved, the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information.”

De-identified data is not PHI

http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
Exceptions – De-identified data

Two methods by which health information can be designated as de-identified:

- Expert Determination § 164.514(b)(1)
  - Apply statistical or scientific principles
  - Very small risk that anticipated recipient could identify individual
- Safe Harbor § 164.514(b)(2)
  - Removal of 18 types of identifiers
  - No actual knowledge residual information can identify individual
Exceptions – De-identified data

All 18 identifiers are removed

(1) Names (including initials);
(2) Street address, city, county, precinct, zip code, and equivalent geo-codes
(3) ALL elements of dates (except year) for dates directly related to an individual and all ages over 89 (this would include procedure dates, date of admission, date of lab work, etc.)
(4) Telephone numbers;
(5) Fax numbers;
(6) Electronic mail addresses;
(7) Social security numbers;
(8) Medical record numbers;
(9) Health plan ID numbers;
(10) Account numbers;
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers/serial numbers;
(14) Web addresses (URLs);
(15) Internet IP addresses;
(16) Biometric identifiers, incl. finger and voice prints;
(17) Full face photographic images and any comparable images; and
(18) Any other unique identifying number, characteristic, or code
Exceptions – Deceased

“Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).”

These data are still PHI
Exceptions – Limited Data Set

- PHI that excludes 16 categories of direct identifiers
- Can use limited data set for research
- Covered entity may disclose limited data set if there is a data use agreement in place first

These data are still PHI

“A covered entity may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing covered entity and the limited data set recipient enter into a data use agreement. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations. Because limited data sets may contain identifiable information, they are still PHI.”

https://privacyruleandresearch.nih.gov/pr_08.asp#8d
Exceptions – Limited Data Set

Data Use Agreement (DUA)
- Specific uses of the limited data set
- Identify who is permitted to receive it
- Specific stipulations on how the data will be used

How do you get a DUA? Who negotiates and signs them?
- Request DUA from Tech Commercialization Office
  - Request a Material Transfer Agreement
  - TCO negotiates and signs DUAs

https://privacyruleandresearch.nih.gov/pr_08.asp#8d
Exceptions – Limited Data Set

**Must exclude:**
- Name
- Address (other than town, city, zip)
- Phone and fax
- Email address
- SSN
- MRN
- Health plan beneficiary numbers
- Account Numbers
- Certificate/license numbers
- VIN
- Device identifiers
- URLs and IP addresses
- Biometric identifiers
- Full face photos
- Any other unique number, characteristic or code that could be used to identify the individual

**May include:**
- City, state and zip code
- Elements of dates related to an individual
  - Date of Birth
  - Admission Date
  - Discharge Date
  - Death Date
Exceptions – Preparatory to Research

“Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. See 45 CFR 164.512(i)(1)(ii). This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.”
Minimum Necessary

“The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.”

Breach Reporting Requirements

When there is a “Breach”

OSU must notify the patient & the Department of Health and Human Services
Breach Reporting Requirements

Disclosure in Violation of HIPAA

Reportable Breach
Unless Low Risk of Compromise

If Reportable

Notify the Patient, OCR, and the Press (if ≥500)
<table>
<thead>
<tr>
<th>Name of OH Covered Entity</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akron General Medical Center</td>
<td>730</td>
<td>11/23/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Central Ohio Urology Group, Inc.</td>
<td>300000</td>
<td>09/23/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Sunbury Plaza Dental</td>
<td>7784</td>
<td>07/21/2016</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Cefalu Eye-Tech of Green, Inc.</td>
<td>850</td>
<td>07/14/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>EDWARD G. MYERS D.O. INC</td>
<td>6441</td>
<td>06/10/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Coordinated Health Mutual, Inc.</td>
<td>591</td>
<td>05/20/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Mayfield Clinic Inc</td>
<td>23341</td>
<td>04/23/2016</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Ohio Department of Mental Health and Addiction Services</td>
<td>59000</td>
<td>04/22/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Edwin Shaw Rehabilitation</td>
<td>975</td>
<td>04/22/2016</td>
<td>Loss</td>
<td>Other</td>
</tr>
<tr>
<td>UHHS Geauga Medical Center</td>
<td>677</td>
<td>03/10/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Community Mercy Health Partners</td>
<td>113528</td>
<td>01/25/2016</td>
<td>Improper Disposal</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Pittman Family Dental</td>
<td>8830</td>
<td>12/31/2015</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>UC Health, LLC</td>
<td>1064</td>
<td>11/14/2015</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
</tbody>
</table>
Increased Enforcement
Office for Civil Rights HIPAA Enforcement

2016: Over $20 Million in Resolution Agreements
2016 Resolution Agreement

Feinstein Institute for Medical Research
- $3.9 million
- Unencrypted laptop stolen from employee’s car
- Disclosed ePHI of 13,000 people
- Lack of risk assessment
- Failed to implement policies, procedures, safeguards
- Three year corrective action plan
Pay Attention To:

Paper
• Shred it
• Binders
• Physical security
• Transportation

Appropriate Approvals

Data Security
Data Security
Security matters…

Maintaining confidentiality matters
• Trust of our patients and research subjects
• Follow laws

There are bad guys who want your data
• Penn State hack
• Ransomware attacks
• PHI is very valuable (think of how a thief could use actual data to bill insurance)
PHI is worth more than credit card information

Medical identify fraud is far worse than financial fraud

<table>
<thead>
<tr>
<th>Medical ID Theft Statistics¹</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of victims total</td>
<td>2.32M</td>
</tr>
<tr>
<td>No. of victims in 2014</td>
<td>500k</td>
</tr>
<tr>
<td>% with out of pocket costs</td>
<td>65%</td>
</tr>
<tr>
<td>Average Out of pocket cost</td>
<td>$13,500</td>
</tr>
</tbody>
</table>

Note: Statistics do not include data from Anthem breach, which could affect up to 80M Americans and impact these numbers greatly

¹ – Ponemon Institute 2014 Survey on Medical Identity Theft, latest year available
Security of HIPAA-protected information must be a part of your data management strategy

So let’s talk about information security at OSU…
OSU Information Security framework

OCIO designed framework to
• Protect our data
• Allow us to comply with the laws governing our data

OCIO in charge of framework, college IT in charge of implementation
• Every college (and even some departments within colleges) has its own approach to the framework

Subset of framework deals with HIPAA-specific security requirements
It all starts with required risk assessment

Key: Follow the data!

Where do the data originate?

Where do the data need to go?

Who can access the data?
Risk assessment applies to vendors as well
Applies to ALL systems holding PHI

The assessment requirement and required security steps also apply to systems that are not managed by IT staff.

Self-developed solutions transfer the responsibility and accountability of security to the researcher/team.
Trade-offs – Determine what works for you

Work Effort Leveraging IT-Provided Tools and Solutions

- Research: 80%
- Administrative: 20%

Work Effort Relying on Self-Developed Tools and Solutions

- Research: 35%
- Database Administration: 10%
- Access Management: 10%
- Encryption: 5%
- Patching: 10%
- Perform Back-ups: 10%
- Administrative: 20%
Where do I start?

- Look at your research and your sponsor requirements
  - Pay attention to requirements at proposal stage – you may be able to budget for security costs

- Are you working with collaborators outside OSU?
  - Are you accessing their PHI, or are they accessing ours?
  - Which data can they access and how?
  - Who is responsible for the data?
  - Who owns the data?
Talk to your IT team

- They can’t help you with your security needs until you tell them about your research and what it entails
  - If IT can’t handle your security, who is?
  - DIY security is not secure
  - Know what your college IT provides before you make promises in proposals
- Have the conversation now!
  - What IT resources, including security, are available?
  - Data security is a finite resource
- Who is *your* IT team?
Common sense security

That Protecting Institutional Data training you’ve been putting off? Take the training to learn more about

• Which data require special protection
• Which IT services you can use with which kinds of data
Question: Can I put my research subject’s name into eRequest to have a check issued to pay the stipend?

Yes

Only if encrypted

No
**Question**: Can I store my HIPAA-protected data on Buckeye Box?

<table>
<thead>
<tr>
<th>Activity</th>
<th>Data Classification</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public</td>
<td>Internal</td>
</tr>
<tr>
<td><strong>SHARE¹</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>OSU Website³</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Portable Storage Media, OSU Managed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Portable Storage Media, Not OSU Managed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Portable Device, OSU Managed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Portable Device, Not OSU Managed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Network Storage, OSU Managed</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>STORE⁴</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Storage, OSU Approved</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cloud Storage, Buckeye Box</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cloud Storage, OneDrive</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Cloud Storage, Others</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Paper</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

*Requires contract through OSU Purchasing and approval of the Security Advisory Board. Then refer to terms of the specific service. For list of OSU approved cloud services, click here.*

*², ⁵, ⁶ refer to specific security guidelines.
Common sense security - encryption

- Databases
- Laptops
- Mobile devices
- Portable storage media

What does it mean for us when encrypted data or devices are lost or stolen?
Common sense security – email

- Email services
  - OSU email
  - Other email services
- Zix
Common sense security – avoiding malware

• **Phishing**
  • Attempt to gain information by posing as a legitimate entity
  • If the email looks fishy, don’t click on links!
  • If you weren’t expecting it, don’t click!
  • Unsure? Send it to your help desk.

• **Malware**
  • Security software can’t stop all attacks
  • Be careful about website ads
  • Don’t open attachment from unknown sources
  • Don’t click on links from unknown sources
Common sense security – ransomware

- Hacker gains access to your data via malware, then locks you out, demanding ransom to restore access
- Prevention is key
  - Limit access to your data
  - Maintain current backup
  - Common-sense anti-malware protection
- If you are attacked, talk to your IT team immediately!
Common sense security – remote access

• What is the best way to access your OSU network remotely?
• Can you use personally owned computers to access PHI?
Suspect a breach of PHI?

- **Immediately** notify your college’s IT director or IT Risk Management if you suspect a problem – do not wait for confirmation
- University has data incident response procedures
  - These procedures go beyond local IT support tasks
Questions?
Who to contact – Arts & Sciences

David Sweasey, Director of IT Risk Management and Governance
614-292-8786
401 Mendenhall Laboratory
Sweasey.1@osu.edu

Andrea R. Ward Ross, Assistant Executive Dean for Research
614-688-4216
ward-ross.1@osu.edu osu.edu
114 University Hall

Sanford L. Shew, Director of Research Computing Services
614-292-9088
Shew.1@osu.edu
406 Mendenhall Lab
Who to contact

Dentistry
Henry Fischbach, Assistant Dean Pre-Doctoral Clinical Operations
fischbach.3@osu.edu
David Savage, Information Systems Director
Savage.63@osu.edu

Nursing
Mary Beth Happ, Associate Dean for Research
614-292-8336
Happ.3@osu.edu
Awais Ali, Director of Information Technology
614-688-5370
Ali.61@osu.edu
Who to contact

Optometry
General help: Contact the Optometry help desk
In person: Geoff Wiggins, Director of Information Technology
614-292-8186
Wiggins.26@osu.edu

Pharmacy
General help: cop-problem@osu.edu
In person: Casey Hoerig, Director of Information Technology
555 Parks Hall
614-292-0408
hoerig.4@osu.edu
Who to contact

Public Health
Don Shymanski, Director of Information Systems
370B Cunz Hall
614-688-4177
shymanski.2@osu.edu