Overview

- HIPAA & Research
- Increased Enforcement
- HIPAA Security
HIPAA & Research
HIPAA & Research

BEYOND THE HIPAA PRIVACY RULE
Enhancing Privacy, Improving Health Through Research

Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, Editors
Committee on Health Research and the Privacy of Health Information:
The HIPAA Privacy Rule

INSTITUTE OF MEDICINE
OF THE NATIONAL ACADEMIES

Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum
National Cancer Policy Forum, Roger Herdman and Harold Moses, Rapporteurs
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
Protected Health Information

(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
Research Requirements

- **Authorization**
  - Specific elements
  - Signed by the patient or personal representative
  - Save for 6 years

- **Waiver of HIPAA Authorization**
  - Factors considered
  - Must save for 6 years
HIPAA Research Authorization Elements

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

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

HIPAA Research Authorization

- Combined with consent
  - “compound authorization”
- Stand-alone
Exceptions

- De-identified
- 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.”
Privacy Rule provides two methods by which health information can be designated as de-identified.

De-Identified

**HIPAA Privacy Rule De-identification Methods**

- **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
De-Identified

(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
Deceased

“Research on Protected Health Information of Decedents. 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).”
Limited Data Set

“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.”
Limited Data Set

- “Date Use Agreement”
  - Specific uses of the limited data set
  - Identify who is permitted to receive it
  - Specific stipulations on how the data will be used.
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:**
- Town, city, state and zip code
- Elements of dates related to an individual
  - Date of Birth
  - Admission Date
  - Discharge Date
  - Death Date
“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.”
“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

- Where there is a “Breach” → We Must Notify the Patient & the Department of Health and Human Services
Breach Regulations

Disclosure in Violation of HIPAA

Reportable Breach
Unless Low Risk of Compromise

If Reportable

Notify the Patient, OCR, and the Press (if >500)
Breach Wall of Shame

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

### Breach Report Results

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</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>Kindred Nursing Centers West, L.L.C.</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1125</td>
<td>09/25/2015</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Sunquest Information Systems</td>
<td>AZ</td>
<td>Business Associate</td>
<td>2100</td>
<td>09/24/2015</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Barrington Orthopedic Specialists, Ltd</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>1009</td>
<td>09/24/2015</td>
<td>Theft</td>
<td>Laptop, Other</td>
</tr>
<tr>
<td>Skin and Cancer Center of Arizona</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>3311</td>
<td>09/21/2015</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
</tbody>
</table>

The Ohio State University
WEXNER MEDICAL CENTER
Increased Enforcement
Office for Civil Rights HIPAA Enforcement: 
Inincreased Enforcement

2016: Over $18 Million in Resolution Agreements
Resolution Agreement

- Feinstein Institute for Medical Research, 2016
  - $3.9 million
  - Unencrypted laptop stolen out of an 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
  - Attention to Binders
  - Physical Security
  - Transport
- Appropriate Approvals
- Data Security
HIPAA Security
Conducting Research Securely

- In a perfect world, you would only need to focus research.

- However, this is not the case, as there are things that come along with research that we need to address:
  - Security Requirements
  - Bad guys – hackers and criminals
  - Errors and failures
Security Requirements

- HIPAA – Protected health information
- FERPA – Student record information
- PCI – Payment card industry
- FISMA – Federal contracts
- FDA – Medical devices
- Joint Commission – Accreditation
- State Laws – Mental health, breach notification
- Other Federal Laws – Chemical dependency; Export Control
- Institutional Standards
  - OSU Information Security Standards (ISS)
  - OSU Information Security Control Requirements (ISCR)
- Industry Standards
Security Requirements

OSU Information Risk Management Program

- Organizational policies, standards, and requirements that address laws and regulations applicable to the university

<table>
<thead>
<tr>
<th>Data Types:</th>
<th>Public</th>
<th>Internal</th>
<th>Private</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. OSU Institutional Data Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. OSU Information Security Standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. OSUWMC Information Security Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. OSU Information Security Control Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Areas:</td>
<td>MGT1-4</td>
<td>PUR1</td>
<td>LEG1</td>
<td>HR1</td>
</tr>
</tbody>
</table>
Security Requirements

OSU Information Risk Management Program

- Security Standard covers 30 identified risk areas
- Specifies security requirements for each area
Security Requirements

Risk Assessments

- In order to protect data when conducting research, we need to understand several things:
  1. Where did the data originate?
  2. Where does the data need to go?
  3. Who can access the data?
Security Requirements

OSU Information Risk Management Program: Risk Assessments

- Certain research may involve vendor systems, third party websites, and/or medical devices obtain, store and maintain data

- To manage information security risk involved, applications and systems need to undergo a risk assessment when implemented

- 4 Goals of a Risk Assessment
  1. Determine and communicate risk of implementing systems in the OSU / OSUWMC environment
  2. Determine and communicate security requirements
  3. Understand the security that is in place for third party systems
  4. Enable presentation of overall system risk profile to OSU / OSUWMC leadership
Security Requirements

Third Party Vendors

- Becoming more and more prevalent in the healthcare and research settings
- Example: Amazon (AWS) and Microsoft (Azure) – IAAS/PAAS/SAAS
- Not all vendors are equal when it comes to information security
Security Requirements

Self-developed vs. IT-provided solutions

- Either may be acceptable if all security requirements are met; however,
- Self-developed solutions transfers the responsibility and accountability of security to the researcher/team.

**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%
- Encryption: 5%
- Access Management: 10%
- Patching: 10%
- Perform Back-ups: 10%
- Administrative: 20%
Bad Guys – Hackers and Criminals

Cyberattack 101: Why Hackers Are Going After Universities

“With their vast stores of personal data and expensive research, universities are prime targets for hackers looking to graduate from swiping credit card numbers.”

“These aren't college kids trying to change their grades. They're potentially nation-state actors much like the hackers who have targeted large corporations in the past.”

“It’s arguably cheaper to try to steal that information than to create it yourself.”

“While the attacks aren't novel, universities don't have strict control over the hardware and software that students and faculty use.”

http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821
Bad Guys – Hackers and Criminals

- PHI is worth more than credit card information
- Medical identity fraud far worse than financial

<table>
<thead>
<tr>
<th>Medical ID Theft Statistics(^1)</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
Bad Guys – Hackers and Criminals

Phishing

- Attempts by hackers/criminals to gain credentials / access to computing resources and/or sensitive data by sending false emails that ask users to do something – typically provide usernames and passwords

Tips:

- Don’t click on links in emails from untrusted sources
- If it’s from a trusted source but still looks suspicious, don’t click
- If the email looks legitimate but you weren’t expecting it, don’t click
- OSU / OSUWMC will never ask to provide your username and password in an email
- If unsure, contact the help desk
Bad Guys – Hackers and Criminals

[Email from Amazon]

Dear Client,

We have sent you this e-mail, because we have strong reason to believe your account has been used in order to prevent any fraudulent activity from occurring we are required to open an investigation.

We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate your account.

To confirm your identity with us click the link below:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,
The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates
Errors and Failures

- Five Case Studies where human error and ineffective information security resulted in breaches and fines.

- Tools to help avoid them.
## OSUWMC Security Tools Review

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Secure Storage</th>
<th>Automated Backups</th>
<th>Secure Collaboration</th>
<th>Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – USB Storage</td>
<td>Encrypting USB devices</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 – SecureMail</td>
<td>Sending restricted data via email</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3 – BuckeyeBox</td>
<td>Approved cloud storage solution</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4 – SharePoint</td>
<td>Secure document storage and collaboration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5 – Shared Drives</td>
<td>Secure file storage and collaboration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>6 – AnyConnect</td>
<td>Automatic remote access to OSUWMC network</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>7 – SecurID Tokens</td>
<td>Remote access to OSU/OSUWMC internal network</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Case #1: Portable Storage Encryption

- Alaska Department of Health and Human Services (DHHS)
- An unencrypted portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHHS employee
- Lead to an investigation by OCR
- $1.7M settlement with HHS in 2012

Case #1: Portable Storage Encryption

- Investigation resulted in findings indicating that DHHS did not:
  - Have adequate policies and procedures in place to safeguard ePHI
  - Have a completed a risk analysis
  - Implement sufficient risk management measures
  - Complete security training for its workforce members
  - Implement device and media controls
  - Address device and media encryption as required by the HIPAA Security Rule.
Case #1: Portable Storage Encryption

OSUWMC Solution / Recommendation – Hardware-encrypted USB Keys

- Alternative media storage solution when primary storage (SharePoint, network drives) is not available
- USB keys and other external storage with restricted data MUST be encrypted
- Acceptable devices - hardware-encrypted, FIPS 140-2 compliant/validated.

![IronKey F200 specifications: multi-factor protection](image)
Case #2: Use of Unauthorized Email Services

- Oregon Health & Science University
- Residents and Dept. of Urology and Kidney Transplant Services used Google Mail and Google Drive to store and share information
- No Business Associate Agreement in place between OHSU and Google
- No settlement but still required notification for >3,000 patients between 2011 and 2013

http://www.ohsu.edu/xd/about/news_events/news/2013/07-28-ohsu-notifies-patients-o.cfm
Case #2: Use of Unauthorized Email Services

OSUWMC Solution / Recommendation – OSUWMC SecureMail

- Secure method of emailing restricted information to individuals external to OSUWMC
- Rather than communicating over unsecured Internet, the message is stored and encrypted on internal servers
- Steps to follow:
  - Include [SECURE MAIL] in subject line
  - External user will receive web link to the message
  - External user will create a SecureMail account to gain access to the message
Case #3: Use of Unauthorized Cloud Services

- St. Elizabeth's Medical Center in Brighton, Mass. (member hospital of Steward Health Care system)
- In 2012, OCR received a complaint from St. Elizabeth’s own employees that the medical center was using a web-based document-sharing application to store PHI
- Upon investigating, OCR determined that SEMC had not thoroughly assessed the security risks to PHI with use of the web application
- $218k settlement and corrective action plan in 2013

Case #3: Use of Unauthorized Cloud Services

OSUWMC Solution / Recommendation – BuckeyeBox

- University-approved cloud storage solution for storing, sharing and accessing files and information from any location
- Approved for Non-Restricted data use;
  - Restricted information, including PHI, is NOT permitted
- Set desired permission levels; Determine who is able to access files
- Must use name.#@osu.edu or first.last@osumc.edu
Case #3: Use of Unauthorized Cloud Services

OSUWMC Solution / Recommendation – **OSUWMC SharePoint sites**

- Team collaboration site; Much more than a file repository
- Storing data is permissible, as is granting access to users external to OSUWMC
- Features include but are not limited to:

<table>
<thead>
<tr>
<th>Collaboration Tools</th>
<th>Search</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Shared documents</td>
<td>• Full-text indexed</td>
<td>• Granular user access controls</td>
</tr>
<tr>
<td>• Document versioning</td>
<td>• Scopes - All Sites or Just this Site</td>
<td>• Access from the Internet</td>
</tr>
<tr>
<td>• check-in/check-out</td>
<td>• You only see what you have permission to see</td>
<td>• Restricted Data</td>
</tr>
<tr>
<td>• Workflows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Calendar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Announcements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Links</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Alerts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case #3: Use of Unauthorized Cloud Services

OSUWMC Solution / Recommendation – Network Shared Drives

- Network storage and collaboration solution
- Simple file repository – drag and drop
- Storing restricted data is permissible – requires appropriate file/folder level restrictions to be implemented
- Accessible externally; Requires SecureID token or AnyConnect software
Case #4: Lost Laptop

- Feinstein Institute – biomedical research institute, sponsored by Norwell Health, Inc.
- In Sept. 2012, reported an unencrypted laptop stolen from employee’s car
- Main findings:
  - (1) lack of encryption; and
  - (2) failure to “implement policies and procedures for granting access to ePHI by its workforce members.”
- $3.9M settlement with HHS and enter into a corrective action plan

http://www.modernhealthcare.com/article/20160318/NEWS/160319891
Case #4: Lost Laptop

OSUWMC Solution / Recommendation – **OSUWMC Managed Laptops & Workstations**

- Per OSUWMC policy, all devices connecting to or storing data from the OSUWMC network must be encrypted.
- In addition, all restricted institutional data – including PHI – must be encrypted.
- To comply with these requirements, personal laptops and workstations must be managed by the organization to ensure encryption and other security tools are encrypted appropriately.
Case #5: Malware - Ransomware

- Hollywood Presbyterian Medical Center
- Ransomware event occurred in February 2016
- Locked workforce members out of many systems, including their EMR, by encrypting files
- Forced to rely on handwritten notes and faxes
- Hackers demanded $3.4M in bitcoins; HPMC paid $17k to have files and systems unlocked
- Many other hospitals have been reporting these kinds of incidents

Case #5: Malware - Ransomware

OSUWMC Solution / Recommendation – YOU

- Anti-malware programs are only so effective; they cannot stop everything
- What we need you to do:
  - For WEBSITES:
    - Be careful about the websites you visit
    - Avoid clicking on website advertisements
  - For EMAIL:
    - Don’t open attachments from unknown senders
    - Don’t click on links from unknown senders
    - Never enter your username and password if requested; If you receive notification that your password is expiring, go to the my.osu.edu site to change it
Case #5: Malware - Ransomware

OSUWMC Solution / Recommendation – **YOU – CONT..**

- Recovery from Incident
  - Do not pay the ransom
  - Depending on how you store your data, recovery may be possible

- Preparation is key
  - Limit access to your folders
  - Maintain current back ups
OSUWMC Solution / Recommendation – AnyConnect

- Allows users with an OSUWMC-managed laptop to automatically connect to the OSUWMC internal network when connecting to the Internet.

- Understand that any time your work laptop is connected to the Internet, you are connected to the OSUWMC network as if you are at your desk. This means that if you leave your device unattended, anyone may gain access to the medical center network.
Case #5: Remote Access Tools

OSUWMC Solution / Recommendation – SecurID Tokens

- Allows authorized users the ability to access the OSU / OSUWMC network from an external location securely.

- Uses a unique and dynamic password that is a combination of:
  1. A known PIN
  2. A one-time password that is generated every 60 seconds

Thank You

- Questions?
- Privacy Office, 293-4477
- Security Office, 293-7672
Appendix / Resources

- Security Processes and Tools Guide

- OSUWMC Information Security Website: https://onesource.osumc.edu/departments/it/informationsecurity/Pages/default.aspx
  - Includes links to
    - OSU Institutional Data Policy
    - OSUWMC Information Security Policy
    - OSU Information Security Standard
    - OSU Information Security Control Requirements