Breaches Happen: Protect Your Patients, Your Research and You

Kathryn Schuff, MD, MCR – Chair, OHSU IRB
John Rasmussen, MA – Chief Information Security Officer
The Intersection of Research and Privacy: Purpose of IRB Review

• To protect the rights and welfare of human subjects involved in research conducted or supported by HHS.

• To protect the rights, safety and welfare of subjects involved in clinical investigations regulated by FDA.
§46.111 Criteria for IRB approval

(1) Risks to subjects are minimized
(2) Risks to subjects are reasonable in relation to anticipated benefits
(3) Selection of subjects is equitable
(4) Informed consent will be sought
(5) Informed consent will be appropriately documented
(6) When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects
(7) When appropriate, there are adequate provisions to *protect the privacy of subjects and to maintain the confidentiality of data*
§50.25 Basic Elements of Consent

(1) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures which are experimental.

(2) A description of any reasonably foreseeable risks or discomforts to the subject.

(3) A description of any benefits to the subject or to others which may reasonably be expected from the research.

(4) A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject.

(5) A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained and that notes the possibility that the Food and Drug Administration may inspect the records.

(6) For research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained.

(7) An explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject.

(8) A statement that participation is voluntary, that refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.
§164.512 Criteria to grant a HIPAA Waiver of Authorization

- The use or disclosure of the PHI involves **no more than minimal risk to the privacy of individuals** based on, at least, the presence of the following elements:
  - **An adequate plan to protect health information identifiers** from improper use and disclosure.
  - An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research
  - Adequate written assurances that the PHI will not be reused or disclosed
Oversight of safety in research studies

...ensuring prompt reporting to the IRB, appropriate institutional officials, and the department or agency head of (i) any unanticipated problems involving risks to subjects or others...

OHRP Example: Lost laptop
Confidentiality of research data

For many studies, the only risk to the research participant is the risk of a breach of confidentiality…

In research, Privacy Matters…
What kind of information are we trying to protect? It’s bigger than research...

- 4 data classifications at OHSU
  - Classified – is US national security data
  - Confidential – patient including research subjects, student, employee information - information protected by law
  - Proprietary - financial information, business plans, unpublished research data, etc.
  - Public

- Same controls to protect all “restricted” information
Items we will cover: on PHI

- Quick reminder – “what is protected health information?”
- Where is the information?
- Use of Cloud Computing platforms and Social Media
- Bring your own device (BYOD)
What is PHI (Protected Health Information)?

• The HIPAA Privacy Rule – 45 CFR § 164.514 (b)(2) lists 18 identifiers plus health information which include:
  – Name, Address, Social Security Number
  – Date of birth, date of service, MRN

• Also includes:
  – E-mail addresses
  – VIN number
  – Serial numbers (implants may have these)
What other rules govern patient information?

- HIPAA/HITECH
- ‘Common Rule’ – 45 CFR 46 as well as FDA law 25 CFR 56
- Oregon Identity Theft Protection Act
- FERPA (student health information)
- Genetic Privacy Laws

- All of these laws are reflected through OHSU policies
PHI and other data is all around us.

- Verbal
- Paper
- Media (wristbands, Rx bottles, X-Ray, etc.)
- Electronic – stored on a wide variety of devices like laptops, smart phones, CD/DVD, tablets, etc.
Don’t forget the paper or printed media...
Don’t leave your printed info behind!

- March 9, 2009
- Massachusetts General Hospital Employee leaves 192 patient charts on the subway
- February 14, 2011
- Mass Gen settles with OCR for $1 million plus a robust corrective action plan

Breach of printed information
The persistence of data – Part 1

• How do you know your data is not on your computing device?
  – If you can access your OHSU email without an Internet connection on your device, that information is stored locally to your computer
  – If you open an attachment from Outlook Web Access on your computer that document is stored in a temporary directory on your device
  – Did you really delete that file?
1) No OHSU Member shall access Electronic Health Information other than by using (a) an OHSU owned or approved and encrypted device or medium; (b) a device that has OHSU approved encryption installed on it; or (c) a device or medium that has an OHSU approved exception.

2) No OHSU Member shall store, download or copy Health Information to any thumb drive, CD or other electronic data storage device or medium that is not encrypted.
What does this mean to me?

• Most OHSU members will be impacted by this policy update over the next 6-9 months.

• Devices that can potentially store, maintain, or transmit PHI will be required to encrypt.
Alaska Department of Health and Human Services

- Thumb drive lost in 2009
- “May have” contained PHI
- Fined $1.7 million
- June 26, 2012

FOR IMMEDIATE RELEASE
June 26, 2012

Alaska settles HIPAA security case for $1,700,000

The Alaska Department of Health and Social Services (DHSS) has agreed to pay the U.S. Department of Health and Human Services’ (HHS) $1,700,000 to settle possible violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. Alaska DHSS has also agreed to take corrective action to properly safeguard the electronic protected health information (ePHI) of their Medicaid beneficiaries.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by Alaska DHSS as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from a vehicle of a DHSS employee. Over the course of the investigation, OCR found evidence that DHSS did not have adequate policies and procedures in place to safeguard ePHI. Further, the evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

In addition to the $1,700,000 settlement, the agreement includes a corrective action plan that requires Alaska DHSS to review, revise, and maintain policies and procedures to ensure compliance with the HIPAA Security Rule. A monitor will report back to OCR regularly on the state’s ongoing compliance efforts.

“Covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices,” said OCR Director Leon Rodriguez. “This is OCR’s first HIPAA enforcement action against a state agency and we expect organizations to comply with their obligations under these rules regardless of whether they are private or public entities.”

OCR enforces the HIPAA Privacy and Security Rules. The Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The Security Rule protects health information in electronic form by requiring entities covered by HIPAA to use physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure.

The HITECH Breach Notification Rule requires entities to report an impermissible use or disclosure of protected health information, or a “breach,” of 500 individuals or more to the HHS Secretary Sebelius and the media. Smaller breaches affecting fewer than 500 individuals must be reported to the secretary on an

Alaska DHSS website: [HHS.gov](http://www.hhs.gov)
In our own back yard...

- 14,000 patient records
- 195 employee records
- Thumb drive stolen from employee home on July 4, 2012
- March 2013 – 4000 OHSU patients notified.
- Their information was stored on an OHSU laptop that was stolen
Use of Social Media for employees

• Posting identified patient information is not permissible

• Before you post any reflections ask yourself “is this information de-identified”?
  – Are dates associated with any postings?
  – Unique situations?
  – Reputationally sensitive information?

• If you are unsure – do not post any information!
Nai Mai Chow – “former” nurse from Gresham

“She was accused of taking graphic photos of patients using bed pans and posting them on Facebook. The pictures date to April 2011.”*

“Chao surrendered her nursing certificate in January and was fired from the Regency Pacific Nursing and Rehab Center in the Portland suburb of Gresham.”

A jury convicted her of an invasion of personal privacy and she spent 8 days in jail plus two years of probation.

*Associated Press - March 7, 2012

Use of Social Media and BYOD
The persistence of data – Part 2

• When using social media tools be careful, once you post something you may never be able to get rid of it.

An active document might be deleted but there may also be a cached version of the information that can be recovered.
Use of Cloud Computing Tools for OHSU Members

- These solutions are generally not permissible for the storage and transmission of PHI and other “restricted” information
  - No privacy for user of this data
  - Company maintains the right to use this information for its own purposes
  - Subject to legal discovery and litigation hold requests
  - Contracts needed to protect data
Avoiding Cloud Computing and Social Media Issues

- Use OHSU resources to securely transmit patient or “restricted” data
  - Epic InBasket for patient communications
  - OHSU email (remember to incorporate treatment information into the EMR)
  - Microsoft Lync for internal IM
  - Telemedicine technologies must be approved prior to use
  - Use “secure:” in the subject line of email to encrypt the message
  - Use H and X drive for storage
Phoenix Cardiology

• From July 3, 2007 until February 6, 2009, Covered Entity posted over 1,000 separate entries of ePHI on a publicly accessible, Internet-based calendar.
• Also transmitted ePHI over Internet based email accounts

Results - April 13, 2012
• $100,000 fine
• Corrective action plan

Use of Cloud Computing

Dr. Fang  Dr. Tibi
Bring your own device (BYOD)

- Personally owned devices are subject to the same policies when used for OHSU business.
- New OHSU policy requires that these devices be approved or encrypted by OHSU prior to use for storage of PHI.
- Under the law information stored on these devices can be subpoenaed by the court.

Filming or Recording on Campus Policy No. 08-30-020
Use of portable and personal devices in a clinical and other environments at OHSU

- Photography of patients for personal purposes is not permissible
- Any photography for treatment purposes must be incorporated into the medical record (this is the provider’s responsibility)
- Images for education must have a signed ROI from the patient prior to photography
The persistence of data – Part 3

- This metadata is often present without you knowing about it.
- Metadata can contain PHI (even if the original document does not).
- Metadata travels with the copy of the electronic data.
By selecting “Properties” under Adobe Reader you can find out all kinds of information about a document.

Some of this may associate to a specific location or a patient.
Is your photo de-identified?

Most smart phones applications will automatically turn on “location services”, this can embed metadata on the photo – Highlighted here are the GPS coordinates of where the photo was taken.

Photo taken on April 1, 2013

Using Picasa we can see the metadata and by clicking the pushpin we can see where the photo was taken.
GPS Coordinates Results

Zooming in with the application we can see that the photo was taken in Sam Jackson Hall.
Consider this before using your personal device…

- Audio and video recording are subject to the same restrictions as photography
- **Your devices must be encrypted if they contain patient information.**
- The loss of these devices must be reported to the Integrity Office as soon as the loss becomes apparent
- **Do not leave these devices unattended in your car (especially if it is the only copy of the data)**
- Only keep the “minimum necessary” stored on a local drive
- Use remote computing tools that keep information off of your device
What do I need to consider if I do not work with patient information?

• Are there export restrictions on your information?

• Is this information patentable? (Patent laws have changed to “first to file”)

• If you work with students or employees, consider their information private
Supplemental Information

• Contact information
• Laws governing the use of patient information and penalties for violations
• Links to OHSU policies
Contact us if you have questions or need to report the loss of information

Report Privacy or Security Concern:
• Integrity Office: 503-494-8849
  – oips@ohsu.edu
  – irb@ohsu.edu
  – Hotline: 877-733-8313 (toll free, anonymous)
  – Enter a report online
• OHSU Public Safety: 4-7744
• ITG Help Desk: 4-2222
Penalties for violations of the law

- Civil monetary penalty (OCR and States)
  - $100 to $1.5 million
- Criminal penalty (personal criminal liability enabled under the HITECH Act)
  - Fines plus jail time
Former UCLA Healthcare Worker Sentenced to Prison for Snooping

- Huping Zhou – cardiothoracic surgeon
- Notified of dismissal from UCLA
- Accessed UCLA records 323 times in one week for celebrities and co-workers
- Sentenced to 4 months in prison
- License revoked


Unauthorized access to PHI