OREGON HEALTH & SCIENCE UNIVERSITY

Lost and Stolen Device and Data.

IRB Brownbag Session, May 22, 2014.

Presented by: John Rasmussen – Chief Information Security Officer
Associate Privacy Officer
OHSU Integrity Office

The goal of this session is to raise awareness of where data might reside and how to protect it.

- Cautionary tales.
- Why we care.
- How we protect our data.

OREGON HEALTH & SCIENCE UNIVERSITY

We'll start with ourselves – July 2012

Stolen thumb drive contained sensitive records from 702 patients at Oregon Health & Science University

By Joe Rojas-Burke, The Oregonian
on July 31, 2012 at 1:43 PM, updated July 31, 2012 at 2:22 PM

Print

After a security lapse, Oregon Health & Science University said it is notifying 702 families that a storage device containing some of their private information was stolen.

A burglar broke into the home of an OHSU employee on July 4 or 5 and stole a briefcase containing a USB thumb drive routinely used to back up data. OHSU said the drive should have been locked in a secure work location and that the employee took it home by mistake.

"In regard to this case, while the stolen USB drive was never intended to leave campus, OHSU has been working to develop methods for ensuring USB drives are encrypted," a statement from the university said. "OHSU plans to step up these efforts in light of this incident."

The drive contained names, dates of birth, phone numbers, addresses, OHSU medical record numbers, and short descriptions of patient medical conditions or family medical histories for about 14,300 premature infant patients. OHSU said most of the data was password-protected. The university is contacting 702 families because only their files contained sensitive personal information that could be used to cause harm, according to Dr. Ronald Marcum, OHSU's chief privacy officer and interim chief integrity officer.

Marcum said OHSU learned of the theft on July 5 but held off notifications until this

Active Discussions

1. Monica Wehby defeats Jason Conger in GOP Senate primary, focuses on Jeff Merkley (election results)
   (429 comments)
2. John Kitzhaber set to run for historic fourth term as Oregon governor (election results)
   (43 comments)
3. Monica Wehby's ex-husband accused her of 'ongoing harassment' during divorce: police report
   (500 comments)
4. Federal investigators issue subpoena to Cover Oregon, Oregon Health Authority
   (108 comments)
5. What would you ask Oregon State's Bob De Carolis, Wayne Tinkle at Beavers' press conference?
   (3 comments)

See more comments »

Most Read

Oregon gay marriage ban struck down by federal judge; same-sex marriages begin

OREGON HEALTH & SCIENCE UNIVERSITY

February, 2013

FAQ: THEFT OF OHSU LAPTOP CONTAINING PATIENT DATA

What exactly was taken?

A laptop computer containing information for 4,022 OHSU patients was recently stolen. The OHSU laptop was taken from an OHSU surgeon's vacation rental home in Hawaii during a burglary on Feb. 22.

How will I know if my information was stolen?

OHSU is sending letters to all impacted patients. We have also set up a toll-free phone line — 1-877-819-9774 — so patients can learn whether their information was impacted. Almost all of the data was for patients who underwent surgery between late 2012 and February 20, 2013.

How likely is it that these families are at risk for identity theft?

OHSU conducted an extensive review of the data in an effort to determine what was taken. While patient health information was contained on the laptop, an analysis revealed there is little to no risk of identity theft for more than 99 percent of the impacted individuals. Records included Social Security numbers for only nine patients.

Are staff allowed to take OHSU laptops home or on vacation?

Yes. Employees are allowed to take OHSU laptops off campus. Policies are in place to protect patient information. In this case, the laptop was protected by password. However, it was not encrypted.

Why wasn't the information encrypted?

All OHSU laptops are password protected, including the laptop stolen during this burglary. However, at the time of this incident, encryption was required only for laptops used for patient care. Because the laptop in question was purchased and used for research purposes, it was not encrypted. Although the physician wrote emails that related to patient care on the laptop, he believed these emails were housed on the OHSU email network – which is secure. However, as is the case with many email programs, recent emails are stored on the computer's hard drive. In an effort to prevent similar issues in the future, OHSU recently enacted even more stringent encryption requirements.

If the theft was on February 22, why didn't you immediately contact families?

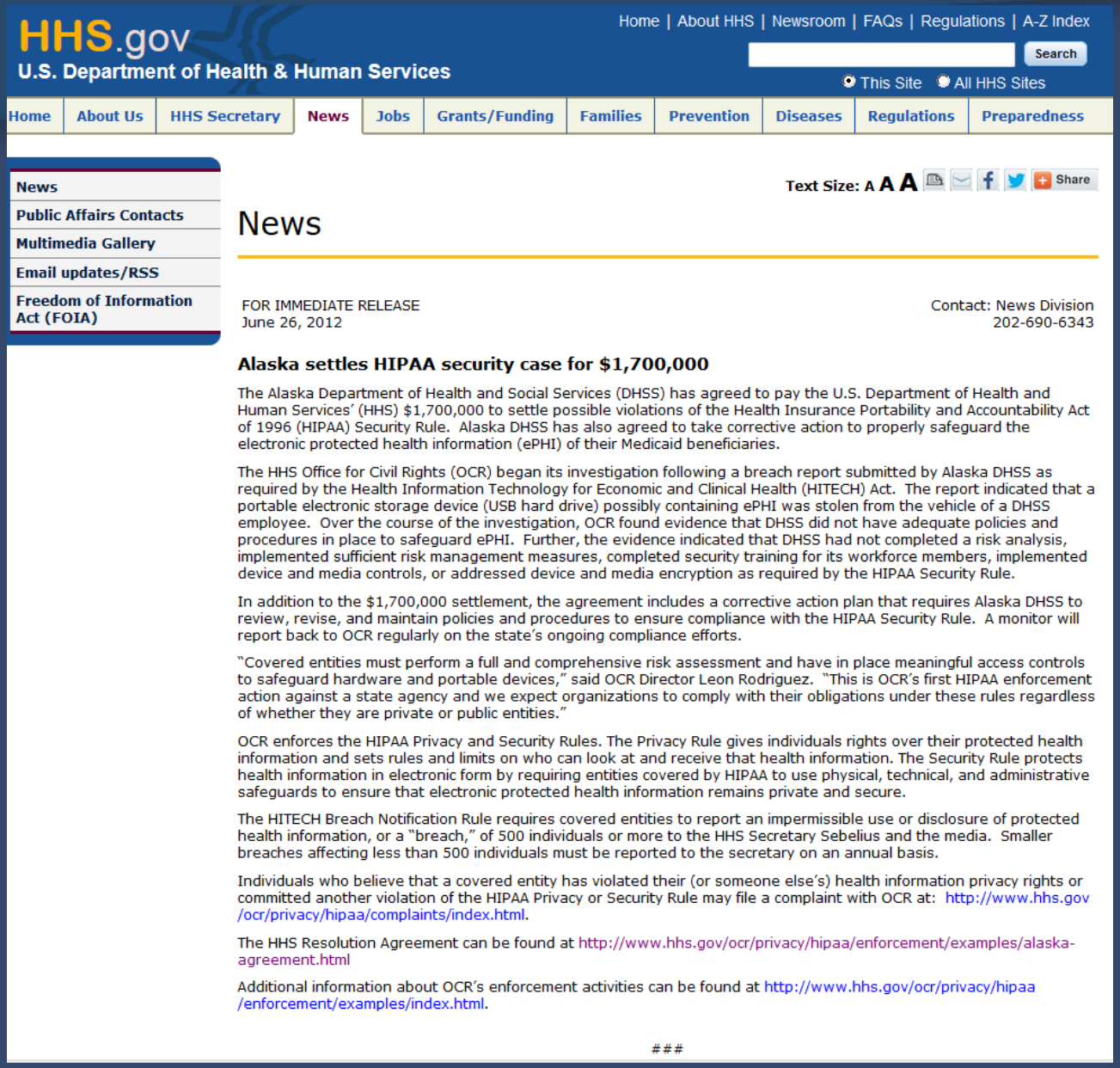
OHSU was unable to immediately contact patients following the theft because there was a significant amount of effort required to determine what was on the stolen computer. OHSU security experts needed to investigate which emails were on the laptop. Then they needed to examine those 5,000 emails individually to identify precisely what data was on the stolen computer and how many people were affected.

Is information security an issue at OHSU?

Patients and physicians have benefitted significantly from recent technology advancements such as electronic records and increased access to email from various locations. However, along with these rapid

OREGON HEALTH & SCIENCE UNIVERSITY

So what? June 2012



HHS.gov
U.S. Department of Health & Human Services

Home | About HHS | Newsroom | FAQs | Regulations | A-Z Index

Search

This Site All HHS Sites

Home | About Us | HHS Secretary | News | Jobs | Grants/Funding | Families | Prevention | Diseases | Regulations | Preparedness

News
Public Affairs Contacts
Multimedia Gallery
Email updates/RSS
Freedom of Information Act (FOIA)

Text Size: A A A Share

News

FOR IMMEDIATE RELEASE
June 26, 2012

Contact: News Division
202-690-6343

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 the 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 covered 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 less than 500 individuals must be reported to the secretary on an annual basis.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

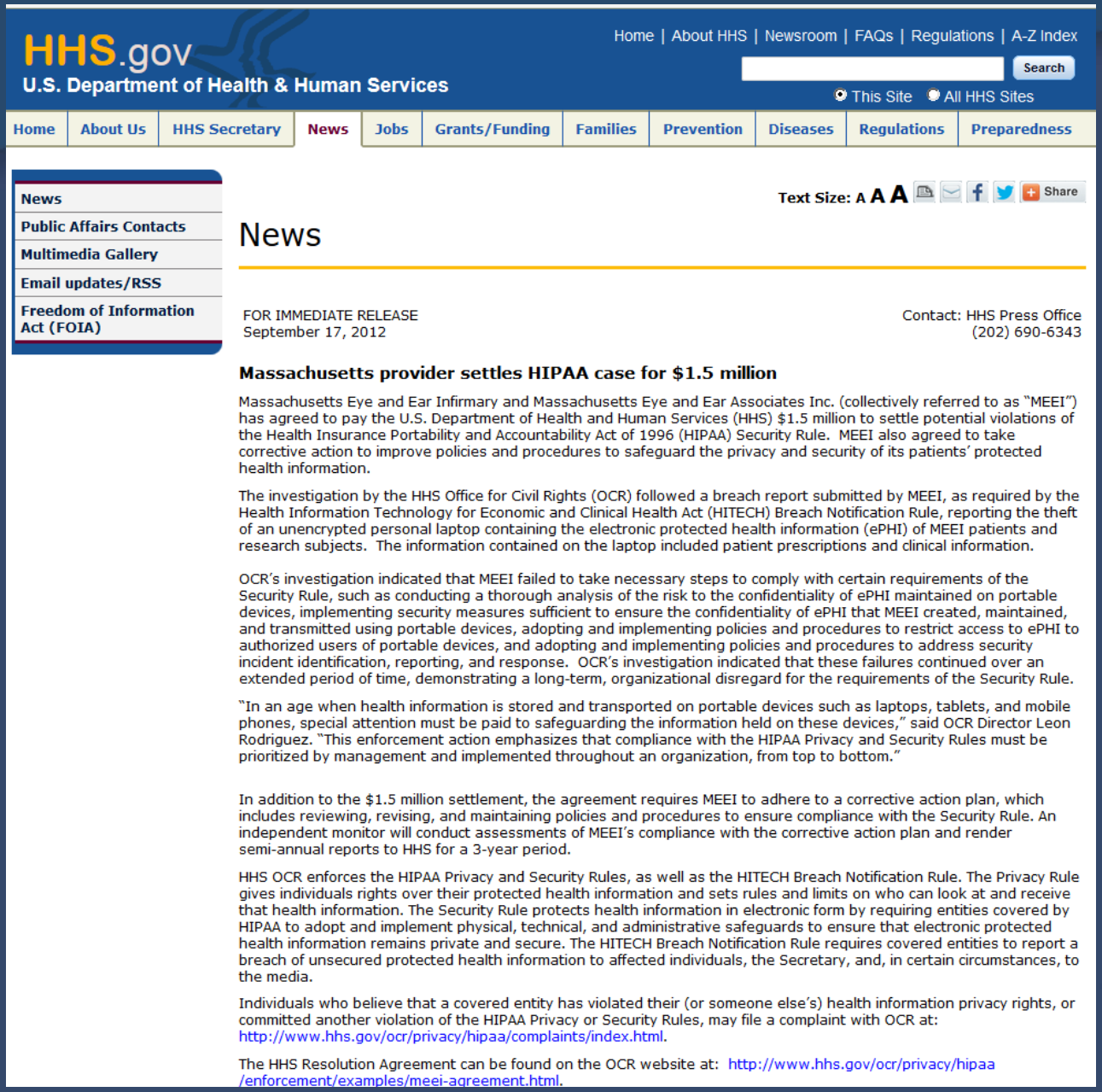
The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

OREGON HEALTH & SCIENCE UNIVERSITY

Maybe it was just a one time thing?



HHS.gov
U.S. Department of Health & Human Services

Home | About HHS | Newsroom | FAQs | Regulations | A-Z Index

Search

This Site All HHS Sites

Home | About Us | HHS Secretary | News | Jobs | Grants/Funding | Families | Prevention | Diseases | Regulations | Preparedness

- News
- Public Affairs Contacts
- Multimedia Gallery
- Email updates/RSS
- Freedom of Information Act (FOIA)

Text Size: A A A Share

News

FOR IMMEDIATE RELEASE
September 17, 2012

Contact: HHS Press Office
(202) 690-6343

Massachusetts provider settles HIPAA case for $1.5 million

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. MEEI also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information.

The investigation by the HHS Office for Civil Rights (OCR) followed a breach report submitted by MEEI, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification Rule, reporting the theft of an unencrypted personal laptop containing the electronic protected health information (ePHI) of MEEI patients and research subjects. The information contained on the laptop included patient prescriptions and clinical information.

OCR's investigation indicated that MEEI failed to take necessary steps to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices, implementing security measures sufficient to ensure the confidentiality of ePHI that MEEI created, maintained, and transmitted using portable devices, adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices, and adopting and implementing policies and procedures to address security incident identification, reporting, and response. OCR's investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule.

"In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices," said OCR Director Leon Rodriguez. "This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom."

In addition to the $1.5 million settlement, the agreement requires MEEI to adhere to a corrective action plan, which includes reviewing, revising, and maintaining policies and procedures to ensure compliance with the Security Rule. An independent monitor will conduct assessments of MEEI's compliance with the corrective action plan and render semi-annual reports to HHS for a 3-year period.

HHS OCR enforces the HIPAA Privacy and Security Rules, as well as the HITECH Breach Notification Rule. 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 adopt and implement physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure. The HITECH Breach Notification Rule requires covered entities to report a breach of unsecured protected health information to affected individuals, the Secretary, and, in certain circumstances, to the media.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights, or committed another violation of the HIPAA Privacy or Security Rules, may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found on the OCR website at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html.

OREGON HEALTH & SCIENCE UNIVERSITY

I’m sensing a pattern…

HHS.gov
U.S. Department of Health & Human Services

Home | About HHS | Newsroom | FAQs | Regulations | A-Z Index

Search

This Site All HHS Sites

Home | About Us | HHS Secretary | News | Jobs | Grants/Funding | Families | Prevention | Diseases | Regulations | Preparedness

- News
- Public Affairs Contacts
- Multimedia Gallery
- Email updates/RSS
- Freedom of Information Act (FOIA)

Text Size: A A A Share

News

FOR IMMEDIATE RELEASE
April 22, 2014

Contact: HHS Press Office
202-690-6343

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

“Covered entities and business associates must understand that mobile device security is their obligation,” said Susan McAndrew, OCR’s deputy director of health information privacy. “Our message to these organizations is simple: encryption is your best defense against these incidents.”

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR’s investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra’s efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR’s investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

OCR received a breach notice in February 2012 from QCA Health Plan, Inc. of Arkansas reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member’s car. While QCA encrypted their devices following discovery of the breach, OCR’s investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and is required to provide HHS with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI. QCA is also required to retrain its workforce and document its ongoing compliance efforts.

OCR has six educational programs for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules. Each of these programs is available with free Continuing Medical Education credits for physicians and Continuing Education credits for health care professionals, with one module focusing specifically on mobile device security: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training

The Resolution Agreements can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health

OREGON HEALTH & SCIENCE UNIVERSITY

Why do we care?

- Consequences.
- Types of information.
- Data likes to hide.

Consequences

- Federal and state laws protect different kinds of information.
- If OHSU stores, transmits, or maintains this kind of information we are subject to these laws and any sanctions.
- Sanctions include
  - fines,
  - corrective action plans,
  - loss of ability to accept credit cards for payment,
  - loss of ability to accept federal financial aid,
  - Criminal penalties!

OREGON HEALTH & SCIENCE UNIVERSITY

There are different types of information we must, or should, protect

- Patient information
- Human subject research information
- Financial information
- Intellectual property
  - Other specially protected information
- Information about our employees
- Student information

OREGON HEALTH & SCIENCE UNIVERSITY

NOTE: OHSU is a public corporation

- OHSU information is subject to public records requests.
- Certain types of information are protected from these requests.
- However, no information should be released unless it is appropriate!

OREGON HEALTH & SCIENCE UNIVERSITY

Type 1, 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
  - Location of service
- Also includes:
  - E-mail addresses
  - VIN number
  - Serial numbers (implants may have these)

What is PHI (Protected Health Information)?

- Health information includes any information about the past, present, or future medical condition of the patient.
- This includes items like:
  - Diagnosis
  - Prescriptions
  - Allergies
  - History
  - Procedure
  - Etc.

OREGON HEALTH & SCIENCE UNIVERSITY

Type 2, Human Subject research information

- Looks a lot like Protected Health Information and since OHSU is a Covered Entity, is subject to the same restrictions.
- Law requires that we treat limited data sets as PHI.

OREGON HEALTH & SCIENCE UNIVERSITY

Type 3, Financial information

- Credit card information
- Budgets
- Business plans
- Chargemaster

OREGON HEALTH & SCIENCE UNIVERSITY

Type 4, Intellectual property

- Grant research
- Privately funded research
- Licensed technologies
- Other institutions licensed technologies (governed by contract)

OREGON HEALTH & SCIENCE UNIVERSITY

Type 5, Employee information

- Employee reviews
- Health information (vaccinations, drug tests, on-the-job injury)
- Salary/bonus information

OREGON HEALTH & SCIENCE UNIVERSITY

Type 6, Student information

- Protected by FERPA.
- Need authorization from student to release any information.

OREGON HEALTH & SCIENCE UNIVERSITY

All kinds of relevant data hides on your computer

- Email information is cached in a special location on the drive for portability.
- Deleted items are not always deleted.
- Cached information is available from web browsing and other applications.
- Meta data may make some information more valuable.

OREGON HEALTH & SCIENCE UNIVERSITY

Is your photo de-identified?

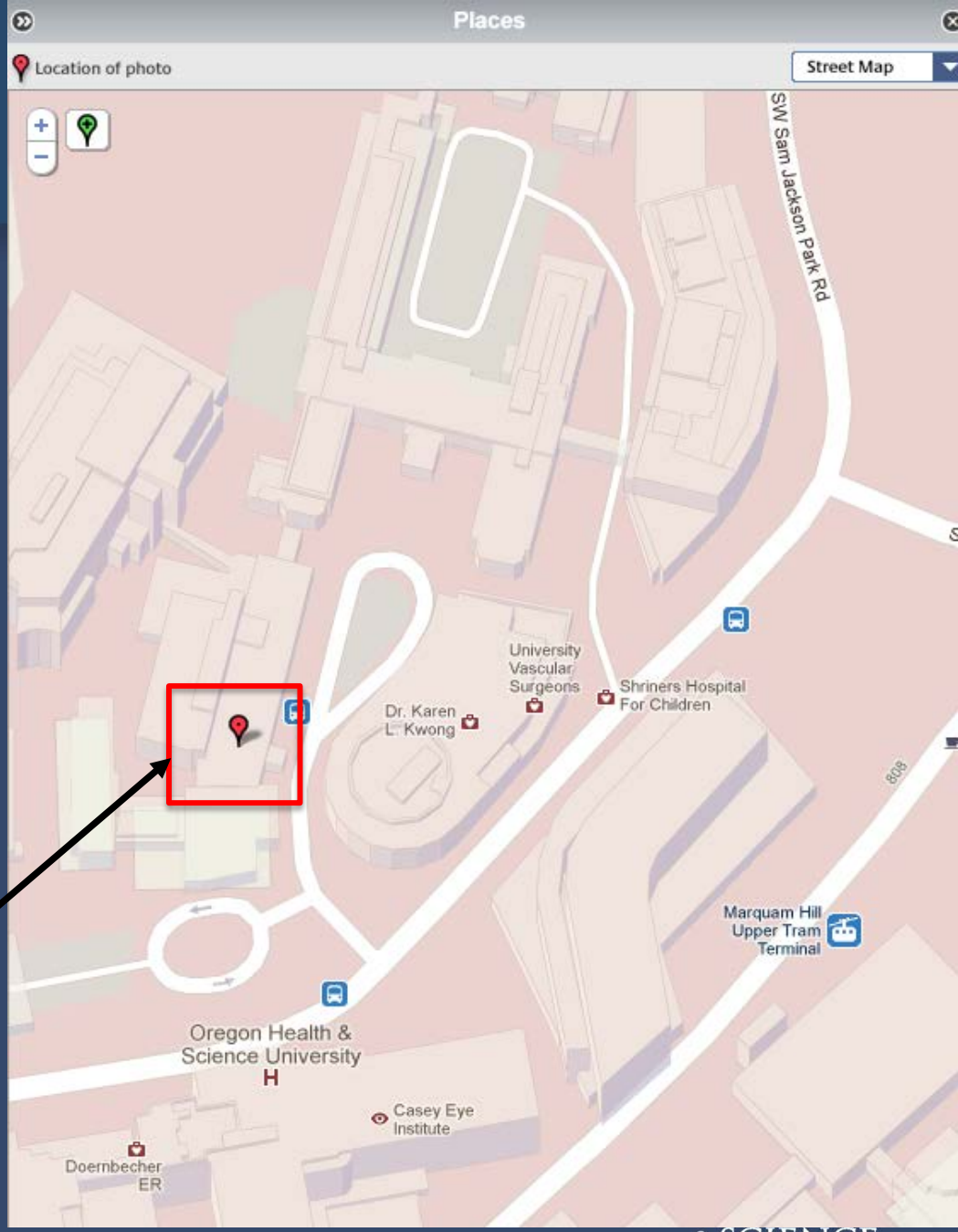
Photo taken on April 1, 2013

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.

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.



&SCIENCE UNIVERSITY

How we protect that data

- Policies – administrative controls
- Physical possession – operational controls
- Encryption – technical controls

*Password protection alone does not protect your information.

OREGON HEALTH & SCIENCE UNIVERSITY

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

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

OREGON HEALTH & SCIENCE UNIVERSITY

Contact us if you have questions or need to report the loss of information

- Report Privacy or Security Concern:
  - Integrity Office
    - 503-494-8849
    - Hotline: 877-733-8313 (toll free and anonymous)
    - Enter a report online
  - ITG Help Desk: 4-2222
  - OHSU Public Safety: 4-7744

OREGON HEALTH & SCIENCE UNIVERSITY