Goals for the session
- To conduct an interactive session with the audience and address security questions and concerns
- Raise awareness of the locations of data
- To define the regulatory requirements and penalties for non-compliance
- Demonstrate ways to protect OHSU data and your own data

What we will cover
- Governance of Information
- Penalties for non-compliance
- Where do we store data?
- Protections for data
- Q&A

Some common terms that may be used...
- Protected Health Information – PHI
- TPO – treatment, payment, health care operations
- Direct treatment relationship
- Disclosure
- Use
- Portable Media
- Electronic Media
- Encryption
How do we classify data?

- OHSU has two high level definitions of data as defined in ISD-700-00001 Information Security Rules.
  - Public
  - Restricted – includes PHI, employee data, student data, research data, business plans, financial data, or any other proprietary OHSU data.

How would you classify this data?

This is public data!

How would you classify this data?

This is OHSU restricted information!

What are your responsibilities?

- OHSU has different classifications for individuals as it pertains to the ownership and responsibility for data.
  - Stewards
  - Users
  - Managers of Users
  - Information Service Providers (a centralized management structure for data services, i.e. ITG)
Stewards
- These individuals have primary responsibility or custodianship of particular information (for example, the Registrar is the steward of student data or a department manager may be the steward of any departmental applications)
  - Risk management
  - Establishing security procedures
  - Assigning and communicating classifications
  - Determining authorizations
  - Reporting incidents
  - Contingency planning
  - Granting authority or responsibility

Users
- Everyone at OHSU is considered a user and are responsible for:
  - Familiarity and adherence to OHSU policy
  - Physical security
  - Secure storage of information
  - Distribution and transmission of data
  - Destruction and disposal of information and devices
  - Logging out, incident reporting, etc.

Managers of Users
- Those with supervisory responsibilities over users. They are responsible for:
  - Establishing security policy and procedures
  - Managing authorizations
  - User training and awareness
  - Incident handling and reporting

Audience poll – which category do you fall in?
- User
- Manager of Users
- Data Steward
- Information Service Provider
- Do you have multiple roles?
Regulations

- HIPAA – Health Insurance Portability and Accountability Act of 1996 (Kennedy-Kassebaum Bill)
  - Title I - health insurance coverage when changing jobs
  - Title II - HIPAA; Administrative Simplification meant to use national standards electronic transactions used in health care
  - HITECH Act - Health Information Technology for Economic and Clinical Health Act
  - Meaningful Use of Electronic Health Records
- Oregon Identity Theft Protection Act
- Genetic Information Nondiscrimination Act (GINA)
- Oregon Genetic law

In addition to patient rights, the HITECH Act requires notification in case of a breach

- Notification for over 500 patients is immediately reported to OCR.
- All patients need to be notified within 60 days of a breach.
- Limited data sets can now require patient notification if they have been breached.

In recent news....

Business Associates are now responsible for implementing HIPAA security controls

- Must implement controls listed in 45 CFR164.308, 310, and 312.
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
- BA’s must notify the covered entity in case of a breach.
Who are some of OHSU’s Business Associates?

Penalties
- Internal – violation of policy
- External – violation of law
  - OCR
  - DOJ
- Civil monetary penalty (OCR and States)
  - $100 to $1.5 million
- Criminal penalty
  - Fines plus jail time

Recent penalties for HIPAA violations
- February 24, Massachusetts General Hospital – $1 million for losing 192 patient records.
- Also applied corrective action plan (CAP) which includes application of new policies and technical controls within 90 days.
- February 22, Cignet Health - $4.3 million for violating patient right to access medical record.

Where do we store data?
- Computing devices
  - Laptops
  - Desktops
  - Smart phones
  - iPads
  - PDA’s
  - Servers
Data on the move

- Portable media
  - CD
  - DVD
  - External storage (the hard drive you bought at Fry’s)
  - Flash drives/thumb drives
  - Disk
  - Tape
  - Media cards

Digital data can leave copies or artifacts where you least suspect

- Microsoft Outlook caches email locally on the computer so you can read your email while travelling.
- Deleted information may not be overwritten and can be recovered.
- Downloading files can leave copies in a variety of locations that you may not be aware of.
- Email can be captured and read without your knowledge.

Now that we’ve scared you...
How do we protect our data?

- Email security:
  - Verify the email address of a recipient before you send "restricted" information.
  - Send "restricted" information through encrypted methods (use "secure:" in the subject line of your email).
  - Do not forward OHSU information to your gmail, Yahoo, Hotmail, or other external account.
  - Do not open messages from people or addresses that you do not know.

Protecting data on your laptop

- Be aware of your physical surroundings, do not leave your laptop on the back seat of your car. (out of sight, out of mind).
- If you have other valuables in your car do not leave them in plain sight. If a thief breaks into your car they will have access to your trunk and unless your laptop is secured to the interior of the trunk it will be stolen.
Protecting data on your laptop

- Use a cable lock when you leave your laptop unattended at OHSU (we have had thefts from private offices).
- Use a password! This is OHSU policy and is the first line of defense for the protection of data.
- Separate work from home. Use your work laptop only for work. Do not let your family use the device.

Encrypt data

- OHSU will soon be distributing full disk encryption to OHSU owned devices. If the device is encrypted there is no way to steal the data if the device is stolen.
- For privately owned devices storing OHSU information use an encryption product to protect sensitive files. (Truecrypt is a good example, and free)

Securing servers and data

- Use ITG or the Advanced Computing Center to host your application. They have processes and procedures in place for backup and security of your data.
- If not centrally managed use NIST 800 series recommendations to secure your data prior to putting it online.

Securing your desktop

- Always lock your desktop when you walk away. Ctrl + Alt + Del and Enter.
- Enable automatic updates for your computer. Do not ignore popups from Adobe or iTunes when they ask you to update. These programs are the primary vector for malware these days.
Portable media

- Physical security is the key...
  - Keep the data in your possession.
  - Maintain an inventory of media storing your data.
- Encrypt data on portable devices. This will be available through the encryption product being pushed by ITG.
- Use device passwords to lock and secure the device.

Internal Contacts

- 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

Web Resources

- OHSU Integrity site: http://www.ohsu.edu/xd/about/services/integrity/
- OCR Privacy site: http://www.hhs.gov/ocr/privacy/
- HHS Breach Reporting Site: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
- Oregon Identity Theft Protection Act: http://www.cbs.state.or.us/dfcs/id_theft.html