THE WHY AND HOW OF DATA SECURITY

YOUR ROLE IN DATA STEWARDSHIP

DEPARTMENT OF MEDICINE IT SERVICES

UW Medicine
DEPARTMENT OF MEDICINE

What is data stewardship?

- Minimizing risk that private information falls into public hands
- Confidential – Protection of data required by law
  - Patient information (PHI) - Protected by HIPAA
  - Student information (FERPA) - Individual Student Records
  - Individual Financial Information - (e.g., credit card, bank) and Personal Information (e.g., social security #, driver's license #) – Protected by Washington state's Personal Information law
  - Personal information (Gotcha!) - (e.g., home address, personal contact information, performance reviews) – Protected by Washington state's public records law
  - Proprietary/research information - Intellectual property or trade secrets – Protected by Washington state's public records law
- Restricted - Data that is not regulated, but for business purposes, is considered protected either by contract or best practice.

Why worry about it?

- Personal consequences
- Professional obligations
- HIPAA reporting cascade
  - All breaches must be reported to feds OCR (Office for Civil Rights investigation)
  - All individuals affected must be notified; if more than 10 lack addresses, public notice on web
  - If more than 500 affected, media must be informed

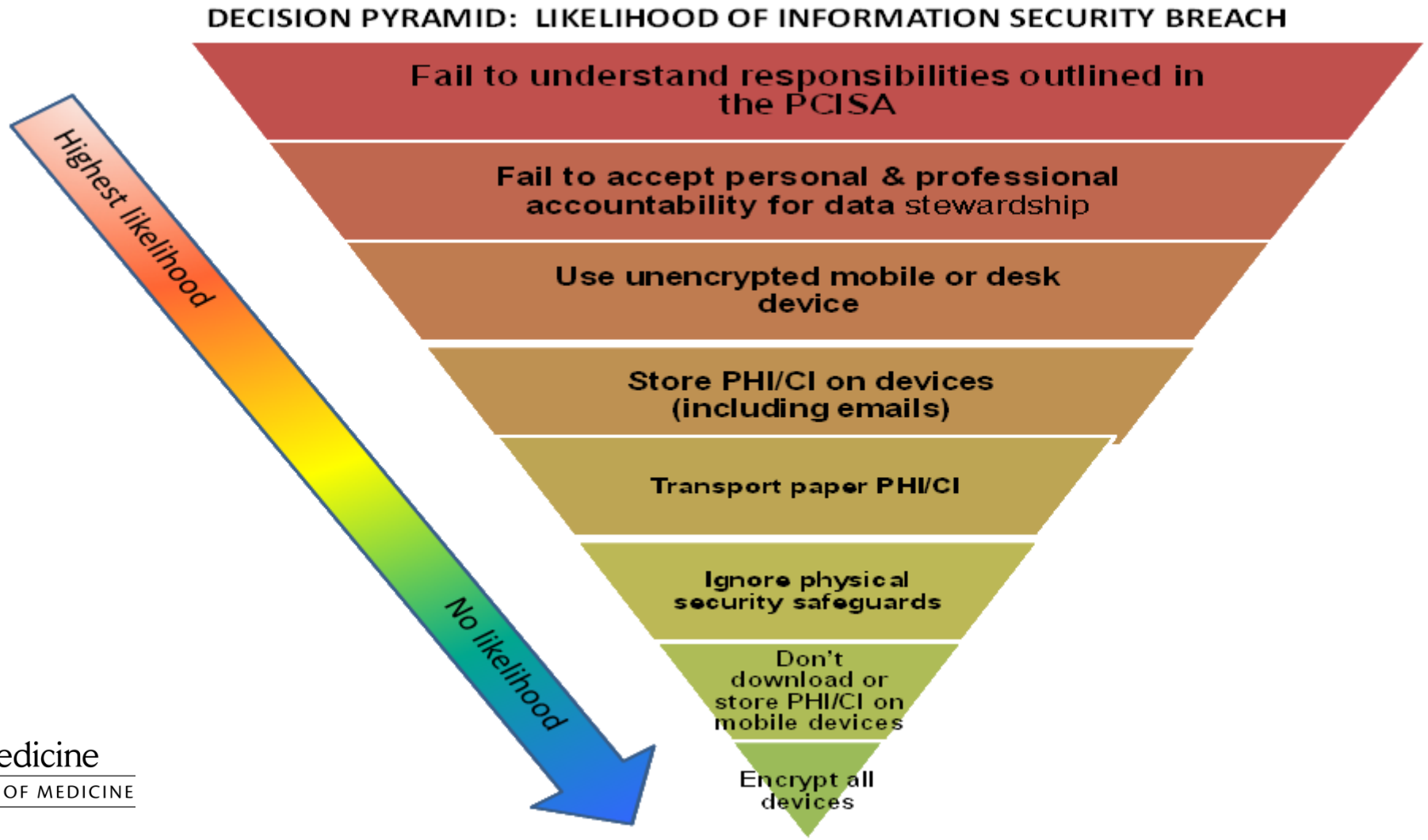
What is a Breach?

- Unauthorized acquisition, access, use, or disclosure of sensitive information that compromises the security or privacy of the information.

- The US Department of Health and Human Services (DHHS) identifies two methods of securing PHI:
  - Destruction
  - Encryption

- No breach occurs if a compromised device is encrypted and password protected.
- If a device is compromised and is not encrypted and password protected, the burden of proof is on you to show there was no confidential data stored on it.

Decision Pyramid: Likelihood of Information Security Breach



Responsibilities

- Everyone who is using or viewing confidential or patient information must be personally and professionally accountable for safeguarding that information.
- Users (YOU) are responsible for the safekeeping of data under your care.
- Minimize your responsibility by limiting the data under your care.

Who to Contact if a Breach Occurs?

- Contact Jennifer Dickey and Walt Morrison if a breach occurs.
  - Jennifer Dickey: jennd@medicine.washington.edu; 221-5947
  - Walt Morrison: wmorrison@medicine.washington.edu; 616-4726

Principle: Data thrift

- Don't be responsible for data you don't need
  - Only store sensitive material on mobile devices if it is absolutely necessary.
- Compute in place:
  - Use internal systems (e.g. ORCA/Epic patient lists) to track information
  - Use institutionally owned servers to store data
  - Utilize the Department of Medicine's NetExtender SSL VPN or AMC's Juniper SSL VPN service for remotely accessing UW resources.
  - Use a terminal server or remote desktop access to your workstation
  - Avoid using computers you are not personally responsible for to access UW resources.
- Can you do it with de-identified information?

Principle: Physical security

- Keep paper and physical documents in a safe place
- Keep computers behind locked doors
- Keep mobile devices close at hand
- Lock computers while unattended.
  - CTRL + ALT + DEL → Enter
  - Windows Key + L

Principle: Encrypted storage

- Encryption: scrambling data so it's practically irretrievable without the key (passphrase)
- All desktop and most mobile operating systems support encryption; many flash drives also include encryption software
- Encryption is only as strong as its passphrase
- "Cloud" storage is generally unsafe and not approved for use unless specifically approved by UW

Principle: Encrypted transport

- A minimally skilled hacker (or moderately skilled lawyer) can read the email you send outside of UW
- "From" addresses can easily be faked
- Secure web connection prevents "listening in", helps verify authenticity of both parties
- VPN, Citrix both good options for enterprise use

Principle: Strong Passwords

- Use the full keyboard.
  - Variety in character types and length makes passwords exponentially stronger.
- Don't use single words or names.
- String multiple random words together to form a long password.
  - Random sentences are a good example.
- A strong password (required by policy) must:
  - Be at least 8 characters long.
  - Mix upper and lower case letters.
  - Include numbers and symbols.

Smartphone/Tablet Security

- Use a strong password to lock the device.
- Enable encryption.
- Set an automatic lockout timer on the device.
  - No greater than 15 minutes.
- Don't use cloud backup services.
  - iOS devices – Use iTunes encrypted backups (http://support.apple.com/kb/HT4946)
  - Android devices – Helium (available in the Play Store)
- Initiate a device wipe after 10 failed password attempts.
  - If the device supports this
- Don't store data on the SIM card (contacts, SMS, etc).

Email Security

- All email containing Restricted or Confidential data must be secured in transport.
  - Encrypted connections must be used between email servers.
- Messages between University email systems (Outpost, UW Exchange, and UW Deskmail) and some recipients are automatically encrypted.
  - This encryption only applies to message data while it moves between servers. It likely will not be encrypted once it reaches its destination mail server.
- Restricted or Confidential information sent over email must be delivered to a secure system.
  - UW Medicine maintains a list of pre-approved email systems on their site: https://security.uwmedicine.org/guidance/technical/email/approved_list.asp.
- Email in Outlook (and other email clients) is cached on the local machine, as are any attachments you open from email messages.
  - This information can be retrieved offline if the local storage of the device is not encrypted.

Key points

- Delete anything sensitive; better yet don't copy it in the first place
- Keep everything you can in a safe place
- Encrypt anything that moves
- Use multiple, secure passwords
- Be suspicious; trust no email
- Spread the word!

Informational Resources

- Discussion Tool / Checklist for Employees https://depts.washington.edu/domweb/forms/IT_PCISADiscussionTool.pdf
- Privacy, Confidentiality and Information Security Agreement for all Employees (part of onboarding process/DoM IT inventory of current users) https://depts.washington.edu/domweb/forms/IT_PCISA.pdf
- UW Medicine Security: https://security.uwmedicine.org/
- The Office of the Chief Information Security Officer for the UW provides resources on their site regarding safe computing - https://ciso.washington.edu/
  - Risk Advisories and Best Practices - https://ciso.washington.edu/resources/risk-advisories/
  - Online Training - https://ciso.washington.edu/resources/online-training/
- A copy of this presentation, as well as technical documentation for securing computers and mobile devices, will be emailed to you.

Where to Get Help

- Department of Medicine IT Services
  - 206.616.8805
  - ishelp@medicine.washington.edu

End of Presentation