HIPAA Security and Research

VALERIE GOLDEN, HIPAA SECURITY OFFICER

Researchers Must Ensure . . .

- Electronic Protected Health Information (ePHI) in their possession or under their control is secured from unauthorized access
- All software or hardware used to access, create, transmit, or store ePHI is secure

HIPAA Security includes:

- Electronic Devices
- Transmission
- Storage and Back-up
- Administrative

How Does Electronic Device Security Impact Research?

- ePHI may only be stored on encrypted devices (includes medical devices)
- Sponsor-owned equipment and software must be secure
- Portable computing devices used for University business must be encrypted – Smart phones, tablets, notebook computers, flash drives, CDs, DVDs, etc.
- University-owned or personally-owned devices are included
- ePHI may not be stored on unencrypted desktops – use the University's secure servers or contact your Tier 1 for secure options

How Do Researchers Know if Electronic Devices are Secure?

- Tier One Support – device encryption assistance
- HSC IT Security – Information Security Risk Assessment
- Include IT Security requirements in Sponsor agreements

I Want to Share the Data with Other Researchers

- ePHI transmitted electronically must be protected from unauthorized access
- ePHI must be encrypted – [secure] in subject line
- Transport Layer Security (TLS) – sender, during transmission, and recipient
- IT Security – List of Email Domains using Secure Connection or TLS Encryption with OUHSC.EDU

I Want to Include ePHI in My Email

- Is it permissible to email ePHI?
- Am I required to use a patient portal?
- Remember the Minimum Necessary Rule
- Do not include PHI in the Subject Line
- [secure]
- Be sure to review the TO field before clicking SEND
- Email sent to an unintended recipient is a HIPAA violation
- Email within the University and to OUMI is secure

Secure Transmission of ePHI

- The method of transmission must be encrypted
  - Email to TLS-enabled business partners
  - Secure File Transfer Protocol
  - Encrypted portable media (flash drive, CD, etc.)
  - Secure interface

I Want to Store my Research Data

- OUHSC's secure servers
- Encrypted portable devices
- OUHSC's Sync & Share

DO NOT STORE ePHI IN

- commercial clouds
- non-OUHSC email accounts
- unencrypted devices

Can HIPAA-Related Research Violations Occur? YES!

SECURITY-RELATED VIOLATION EXAMPLES

- Auto-forwarded emails to personal email account
- Stolen unencrypted laptops
- Lost unencrypted flash drives
- Lost iPhone with a weak password (1234)
- Employee allowed bogus external support to access her phone and shared OUHSC credentials with them
- Unsecure website used to schedule appointments for free services
- Sent PHI via unsecure text message
- Lost office keys and badges

MD Anderson to pay $4.3M

MD Anderson was required to pay $4,348,000 in civil money penalties to OCR for HIPAA violations:

-lost unencrypted laptop containing research ePHI

-lost unencrypted flash drives containing research ePHI

Fourth largest amount ever awarded to OCR by an ALJ or secured in a settlement for HIPAA violations – more than $25M awarded in 2018!

***Report stolen unencrypted devices to HIPAA Team and to IT Security as soon as possible so we can begin mitigation efforts!!!

Final Reminders

- Review and comply with the HIPAA Privacy and Security Policies
- Secure the PHI you possess/control
- Never store ePHI on an unencrypted device or in a cloud
- Always use [secure] to email ePHI outside of OUHSC
- Ensure sponsor-owned devices are secure (ask IT!)
- Always keep portable devices physically secure to prevent theft and unauthorized access

When in Doubt – ASK!!!

- OUHSC Compliance Website
  HIPAA – http://www.ouhsc.edu/hipaa

- University Privacy Official
  jill-raines@ouhsc.edu

- HIPAA Security Officer
  valerie-golden@ouhsc.edu

- HIPAA Compliance Auditor
  mary-Milano@ouhsc.edu

- Compliance Hotline
  (405)271-2233
  (866)836-3150

QUESTIONS???