HIPAA TECHNOLOGY COMPLIANCE

College of Nursing

WHAT IS HIPAA?

- HIPAA is an acronym for Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164).
- It provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.
- Each Part of HIPAA is governed by different laws.
- Three Aspects: 1. Privacy Rule; 2. Security Rule; 3. Electronic Data Exchange.

HIPAA PRIVACY RULE

- Privacy Rule went into effect **April 14, 2003**.
- Privacy refers to protection of an individual's health care data.
- Defines how patient information used and disclosed.
- Gives patients privacy rights and more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

HIPAA SECURITY RULE

- Security (IT) regulations went into effect **April 21, 2005.**
- Security means controlling:
  - **Confidentiality** of electronic protected health information (PHI).
  - **Storage** of electronic protected health information (PHI)
  - **Access** into electronic information

HIPAA ELECTRONIC DATA EXCHANGE (EDI)

- Defines transfer format of electronic information between providers and payers to carry out financial or administrative activities related to health care.
- Information includes coding, billing and insurance verification.
- Goal of using the same formats is to ultimately make billing process more efficient.

WHY COMPLY WITH HIPAA?

- To show our commitment to protecting privacy
- As an employee, you are obligated to comply with State, University, and College security policies and procedures
- Our patients/research participants/members are placing their trust in us to preserve the privacy of their most sensitive and personal information
- Compliance is not an option, it is required.
- **If you choose not to follow the rules:**
  - ❖You could be put at risk, including **personal** penalties and sanctions
  - ❖You could put the College at risk, including financial and reputational harm

WHY IS PRIVACY AND SECURITY TRAINING IMPORTANT?

- It outlines ways to prevent accidental and intentional misuse of PHI.
- It makes PHI secure with minimal impact to staff and business processes.
- It's not just about HIPAA – it's about doing the right thing!
- It shows our commitment to managing electronic protected health information (PHI) with the same care and respect as we expect of our own private information. It is everyone's responsibility to take the confidentiality of patient information seriously.
- Anytime you come in contact with patient information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations.
- The law requires us to train you.
- To ensure your understanding of the Privacy and Security Rules as they relate to your job.

HIPAA DEFINITIONS

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

- Protected Health Information (PHI) is individually identifiable health information that is:
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse and that
    - ❖ Relates to the past, present, or future physical or mental health or condition of an individual;
    - ❖ Relates to the provision of health care to an individual
    - ❖ The past, present or future payment for the provision of health care to an individual.

HIPAA DEFINITIONS

PHI DEFINITION CONTINUED….

PHI includes information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. PHI is defined as data in an electronic format that contains any of the 18 identifiers

This may include but is not limited to the following:

- Data stored on the network, internet, or intranet
- Data stored on a personal computer or personal digital device i.e. Cell Phone
- Data stored on "USB keys," memory cards, external hard drives, CDs, DVDs, or digital cameras/camcorders
- Data stored on your HOME computer
- Data utilized for research

HIPAA DEFINITIONS

WHAT CONSTITUTES PHI – EIGHTEEN IDENTIFIERS

- Name
- Address -- street address, city, county, zip code (more than 3 digits) or other geographic codes
- Dates directly related to patient
- Telephone Number
- Fax Number
- email addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL, Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)
- Age greater than 89 (due to the 90 year old and over population is relatively small)

HIPAA SECURITY STANDARDS

WHAT CAN I DO TO HELP PROTECT OUR COMPUTER SYSTEMS AND EQUIPMENT?

- Workstation use
  - Restrict viewing access to others
  - Follow appropriate log-on and log-off procedures
  - Lock your workstation, press Ctrl-Alt-Del or Windows key + "L"
  - Use automatic screen savers that lock your computer when not in use
- Please check with CON IT before installing any software.
- Know and follow organizational policies
- If devices are lost, stolen or compromised, notify CON IT immediately!
- Do not store PHI on mobile devices unless you are authorized to do so and appropriate security safeguards have been implemented.

HIPAA SECURITY STANDARDS

ACCESS -USERNAMES AND PASSWORDS

- Passwords must be changed every 180 days.
- Passwords should be changed whenever there is a question of compromise.
- Strong passwords must be utilized.
  - A minimum of 8 characters in length
  - Should contain a component from each of the 4 following categories
    - Upper case
    - Lower case
    - Numerals
    - Keyboard symbols
- Use a “pass-phrase” such as MbcFi2yo (My brown cat Fluffy is two years old) instead of passwords that others may be able to guess (i.e. Spouse/Pet/Child Names, Dates, Sports Teams)

HIPAA SECURITY STANDARDS

REMOTE/OFF CAMPUS ACCESS

- All PHI stored or accessed remotely must be maintained under the same security guidelines as for data accessed within the College of Nursing network.
- This applies to home equipment and Internet-based storage of data.
- All PHI should be kept in such a fashion as to be inaccessible to family members or other unauthorized individuals.
- Stored data should be appropriately encrypted.

HIPAA SECURITY STANDARDS

E-MAIL SECURITY

Appropriate use of e-mail can prevent the accidental disclosure of PHI. Some tips or best practices include:

- Use email in accordance with policies and procedures defined by the University of South Carolina.
- Use e-mail for business purposes and do not use e-mail in a way that is disruptive, offensive, or harmful.
- Verify email address before sending.
- Use <encrypt> brackets in the SUBJECT line to encrypt sensitive email data.
- Include a confidentiality disclaimer statement.
- Don’t open e-mail containing attachments when you don’t know the sender.

HIPAA SECURITY STANDARDS

ADMINISTRATIVE – MALICIOUS SOFTWARE

Emails with attachments should not be opened if:

– The sender is unknown to you

– You were not expecting the email/attachment

– The attachment is suspicious in any way.

– Do not open non-business related email attachments or suspicious web URLs.

– Do not open file attachments or URLs sent via instant messaging or text.

HIPAA SECURITY STANDARDS

EMAIL ENCRYPTION PROCEDURE FOR OFFICE 365

Encryption ensures that protected or sensitive information remain private during email transmission. This protects the individual and the university from potentially costly and reputation-damaging data breaches.

Any university email that contains the following protected or sensitive information must be encrypted:

- Protected health information [PHI] (i.e., patient record information, etc.)
- Personally Identifiable Information [PII] (i.e., Social Security Number, specific identity information, etc.)
- Credit card information
- Any information protected by governmental or institutional regulations

How to encrypt an email message

To send an encrypted message, use the encryption trigger **encrypt with brackets** (see options below) in the Subject line of the email message and send the message normally.

<encrypt>, (encrypt), [encrypt], or {encrypt}

The encryption trigger is NOT case sensitive

University of South Carolina

HIPAA SECURITY STANDARDS

INFORMATION ACCESS – CON RESEARCH SERVER

- Access to the College of Nursing Research AWS server is granted only to authorized individuals with a "need to know."
- College of Nursing computer equipment should only be used for authorized purposes in accomplishing your specific duties.
- Disclosure of PHI via electronic means is strictly forbidden without appropriate authorization.
- Do not store data from the AWS server on your desktop or on any device that is not encrypted.
- Faculty who terminate their employment must advise CON IT that PHI data has been destroyed or transferred.

HIPAA SECURITY STANDARDS

PHYSICAL SAFEGUARDS

- Physical Safeguards is defined by "the security measures to protect a covered entity's electronic health information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion."
- Bottom Line:
  - **Electronic assets must be protected from physical damage and theft**

HIPAA SECURITY STANDARDS

PHYSICAL –SERVER, MEDIA AND DEVICES

- All applicable CON electronic media containing PHI should be marked as confidential and properly encrypted.
- Do not save any documents containing PHI to a workstation desktop
- Do not save any documents containing PHI to any device that is not encrypted
- Do not save any documents containing PHI to your "documents" folder on your computer or the K Drive. You are permitted to save them to OneDrive For Business (not personal OneDrive) or the CON Research Server only.
- OneDrive for Business storage should be used as a **temporary** measure for storing and transferring PHI. There is a limited amount of data that may be stored and is deleted when you leave the university. For these reasons **it should not be used for long term data storage**.
- Electronic devices containing PHI should be secured behind locked drawers, cabinets, or doors when applicable.

HIPAA SECURITY STANDARDS

PHYSICAL MEDIA & DEVICES

- Special security consideration should be given to portable devices (laptops, smartphones, digital cameras, digital camcorders, external hard drives, CDs, DVDs, USB flash drives, and memory cards) to protect against damage and theft.
- At no time should PHI be stored on any mobile device unless the data is properly encrypted.

HIPAA SECURITY STANDARDS

PHYSICAL - WORKSTATIONS

- Workstations must be positioned so as to avoid viewing by unauthorized personnel.
- Use privacy screens where applicable.
- Use automatic password protected screen savers.
- Lock, logoff or shut down workstations when not attended.
- Workstation access should be controlled based on job requirements.

HIPAA SECURITY STANDARDS

PHYSICAL – INFORMATION DISPOSAL

- Disposal of electronic data must be done in such a fashion as to ensure continued protection of PHI.
- Magnetic media must be erased with a degaussing device or approved software designed to overwrite each sector of the disk. This must be done prior to disposal or reuse.
- CDs and DVDs must be broken, shredded, or otherwise defaced prior to being discarded. •
- All media containing PHI must be disposed of in compliance with the University Electronic Data Disposal Policy.

HIPAA SECURITY STANDARDS

ADMINISTRATIVE - ACCESS

Employee Termination and/or transfer procedures:

- –Administrative directors are responsible for informing the appropriate IT administrator of changes in an employee's employment status. **Faculty should notify the Nursing Helpdesk when a student assistant with server access has ended their employment**.
- –Upon termination of employment all USC network and PC access is terminated.
- –All PHI and computer equipment (laptops, tablets, etc.) should be retrieved.
- –The use of a prior employee's user-ids and passwords is strictly forbidden.

HIPAA SECURITY STANDARDS

INCIDENT RESPONSE – DATA BREACH

- All known and suspected security violations must be reported.
- Security incidents should be reported to the departmental Administrative Director or their designee.
- CON IT personnel should be contacted immediately to initiate the appropriate investigative processes and to mitigate against any data loss.
- Security incidents must be fully documented to include time/date, personnel involved, cause, mitigation, and preventive measures.

HIPAA SECURITY STANDARDS

DISCOVERY OF BREACH

- A breach is treated as discovered:
  - On first day the breach is known to the covered entity, or
  - In the exercise of reasonable diligence, it should have been known to the covered entity.
- Notification time period for a breach begins when the organization did or should have known it existed

BREACH NOTIFICATION RULE

DEFINITION OF BREACH (45 C.F.R. 164.402)

- Impermissible use or disclosure of (unsecured) PHI is assumed to be a breach unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised based on a risk assessment.
- Unsecured PHI: "Unsecured protected health information" means protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology required by the Breach Notification Rule.

BREACH NOTIFICATION

RISK ASSESSMENT FACTOR #1

If you suspect there has been a data breach, you must perform a risk assessment. Evaluate the nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification of the PHI:

- Social security number, credit card, financial data (risk of identity theft or financial or other fraud)
- Clinical detail, diagnosis, treatment, medications
- Mental health, substance abuse, sexually transmitted diseases, pregnancy

BREACH NOTIFICATION

RISK ASSESSMENT FACTOR #2

- Consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made:
    - Does the unauthorized person who received the information have obligations to protect its privacy and security?
    - Is that person workforce of a covered entity or a business associate?
    - Does the unauthorized person who received the PHI have the wherewithal to re-identify it?

BREACH NOTIFICATION

RISK ASSESSMENT FACTOR #4

- Consider the extent to which the risk to the PHI has been mitigated:
  - Example: Obtain the recipient's satisfactory assurance that information will not be further used or disclosed
    - Confidentiality Agreement
    - Destruction, if credible
    - Reasonable Assurance

BREACH NOTIFICATION

RISK ASSESSMENT FACTOR #3

- Consider whether the PHI was actually acquired or viewed or if only the opportunity existed for the information to be acquired or viewed
- Example:
  - Laptop computer was stolen, later recovered and IT analysis shows that PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised
  - The entity could determine the information was not actually acquired by an unauthorized individual, although opportunity existed

BREACH NOTIFICATION

RISK ASSESSMENT CONCLUSION

- Evaluate the overall probability that the PHI has been compromised by considering all the factors in combination (and more, as needed)
- Risk assessments should be:
    - Thorough
    - Performed in good faith
    - Conclusions should be reasonably based on the facts
- If evaluation of the factors fails to demonstrate low probability that the PHI has been compromised, **breach notification is required**

HOW DO PRIVACY VIOLATIONS HAPPEN?

- **Fax Document to Wrong Location**
  - "Hello, this is Pizza Plaza on Stark Street. Did you mean to fax me this lab result for Fred Flintstone?"

- **Sending an unencrypted email that contains PHI**
  - "I forgot to put the brackets in the header of Wilma's e-mail."

- **Forgetting to Verify Patient Identity**
  - "There were seven patients with the name Barney Rubble. I should have confirmed his date of birth."

SUMMARY

- **You** are the most important component of IT security.
- Be mindful of security requirements and your responsibility to protect proprietary research subject and patient information.
- Report any suspicious activities or concerns to the Nursing Helpdesk at 777-1213
- Contact the Nursing Help Desk for any questions or assistance.

IT SECURITY CONTACTS

- **Ryan Webber:** rwebber@mailbox.sc.edu, 777-3756
- **Rachel Coleman:** reliving@mailbox.sc.edu, 777-2028
- **Nursing Helpdesk:** nurshd@mailbox.sc.edu, 777-1213

THANKS!

REFERENCES:
HIPAA COLLABORATIVE OF WISCONSIN
USC SCHOOL OF MEDICINE

Rachel Coleman

IT Support Specialist III

reliving@mailbox.sc.edu

803-777-2028

South Carolina