



# HIPAA Technology Compliance

UNIVERSITY OF SOUTH CAROLINA  
COLLEGE OF NURSING

# 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

WHAT IT IS AND HOW IT WORKS

# 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.
- ▶ There are three aspects of HIPAA:
  - ▶ Privacy Rule
  - ▶ Security Rule
  - ▶ Electronic Data Exchange



# HIPAA Privacy Rule



The Privacy Rule went into effect April 14, 2003.



Privacy refers to protection of an individual's health care data.



Defines how patient information is used and disclosed.



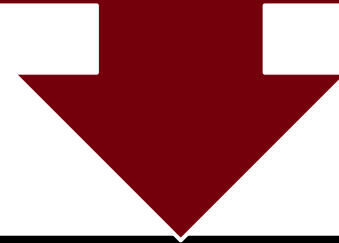
Gives patients privacy rights and more control over their own health information.



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 do we have to comply?

- ▶ Because we are a covered entity
- ▶ 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 University/College at risk, including financial and reputational harm





# PHI –Protected health information

WHAT IS IT AND HOW DO WE PROTECT IT?

# 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.
- ▶ ePHI or Electronic Protected Health Information is patient health information which is computer based, e.g. created, received, stored or maintained, processed and/or transmitted in electronic medial.
- ▶ Electronic Media includes computers, laptops, disks, memory sticks/usb drives, cell phones, tablets, servers, networks, e-mail, websites, etc.

# What is Protected Health Information (PHI)

▶ 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

# What is **not** PHI

- ▶ In contrast, some research studies may use health-related information that is personally identifiable because it includes personal identifiers such as name or address, but it is not considered to be PHI because the data are not associated with or derived from a healthcare service event (treatment, payment, operations, medical records) and the data are not entered into the medical records. HIPAA does not apply to “research health information” (RHI) that is kept only in the researcher’s records; however, other human subjects protection regulations still apply.
- ▶ Examples of research using only RHI and thus not subject to HIPAA include: use of aggregated (non-individual) data; diagnostic tests from which results are not entered into the medical record and are not disclosed to the subject; and testing conducted without any PHI identifiers. Some genetic basic research can fall into this category, such as the search for potential genetic markers, promoter control elements, and other exploratory genetic research. In contrast, genetic testing for a known disease, as part of diagnosis, treatment, and health care, would be considered a use of PHI and therefore subject to HIPAA regulations.
- ▶ Also note, health information by itself without the 18 identifiers is not considered to be PHI. For example, a data set of vital signs by themselves does not constitute protected health information. However, if the vital signs data set includes medical record numbers, then the entire data set is considered PHI and must be protected since it contains an identifier.

# 18 PHI Identifiers (1-9)

- ▶ 1. Names;
- ▶ 2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- ▶ 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- ▶ 4. Phone numbers;
- ▶ 5. Fax numbers;
- ▶ 6. Electronic mail addresses;
- ▶ 7. Social Security numbers;
- ▶ 8. Medical record numbers;
- ▶ 9. Health plan beneficiary numbers;

## 18 PHI Identifiers (10-18)

- ▶ 10. Account numbers;
- ▶ 11. Certificate/license numbers;
- ▶ 12. Vehicle identifiers and serial numbers, including license plate numbers;
- ▶ 13. Device identifiers and serial numbers;
- ▶ 14. Web Universal Resource Locators (URLs);
- ▶ 15. Internet Protocol (IP) address numbers;
- ▶ 16. Biometric identifiers, including finger and voice prints;
- ▶ 17. Full face photographic images and any comparable images; and
- ▶ 18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

# PHI Identifiers

- ▶ There are also additional standards and criteria to protect individuals from re-identification. Any code used to replace the identifiers in data sets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed.
- ▶ For example, a subject's initials cannot be used to code their data because the initials are derived from their name.
- ▶ Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.

## Viewing and accessing PHI for unauthorized reasons is prohibited

1

It is never acceptable to look at PHI “just out of curiosity,” even if no harm is intended, e.g., finding an address to send a ‘get well’ card, or looking up a neighbor or co-worker’s diagnosis.

2

There is no difference if the information relates to a “high profile” person, close friend, or family member – ALL information is entitled to the same protection and must be kept private.

3

Improper use or disclosure of PHI presents risks of

- Identify theft
- Invasion of privacy
- Harm
- Embarrassment to students, faculty, staff, patients, research participants, and the University



# Prevent PHI from being compromised

PHI is compromised when it is not properly stored or secured or is subject to nefarious acts such as malware or phishing attempts. PHI is also compromised when it is lost, stolen, improperly disposed of, or communicated to unauthorized persons.

## **EXAMPLES**

- ▶ Not knowing the location of paper records or a device containing PHI
- ▶ System containing PHI is hacked or PHI is accessed in a PHISHING scheme
- ▶ Gossiping about information learned from a medical record
- ▶ Sending PHI to the wrong address (mail or email)
- ▶ Auto forwarding email to a personal or other unauthorized account
- ▶ Sharing a folder on a cloud system (OneDrive) with someone not authorized to see PHI in the folder
- ▶ Not properly securing a folder on One Drive to prevent unauthorized viewing of PHI in the folder

## Top 15 Examples of HIPAA Violations

01



Employees  
Divulging Patient  
Information

02



Medical Records  
Falling into the  
Wrong Hands

03



Stolen Items

04



Lack of Proper  
Training

05



Texting Private  
Information

06



Passing Patient  
Information  
Through Skype  
or Zoom

07



Discussing  
Information  
Over the Phone

08



Posting on  
Social Media

09



Employees  
Accessing Files  
and Patient  
Charts Without  
Authorization

10



Using PHI for  
Personal Gain

11



Written Consent

12



Home  
Computers

13



Inquiries in  
Social Settings

14



Poor Reporting  
Timing

15

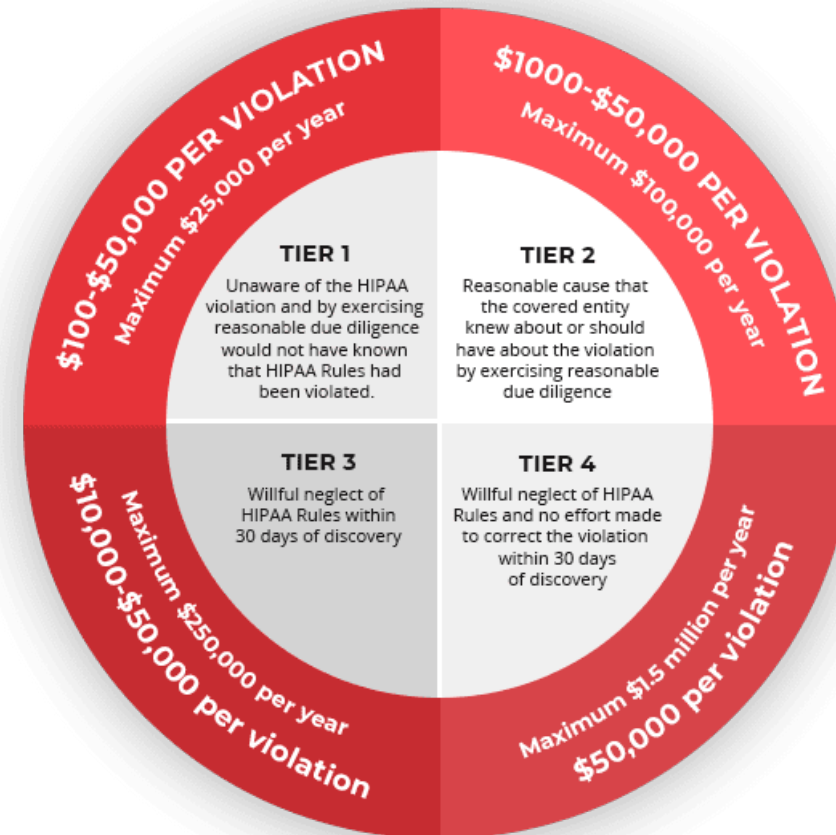


Releasing  
Records After  
Authorization  
Date

# Disciplinary action

- ▶ If you violate HIPAA or University Policy, you will be subject to appropriate disciplinary action as outlined in the University's policies, standards, and guidelines.
- ▶ You may also be subject to criminal or civil penalties.

## HIPAA Violation Penalties



Access -Usernames and Passwords

Remote/Off-Campus Access

Email Security

Email Attachments

Email Encryption for Microsoft 365

Physical Safeguards

Information disposal

# HIPAA Security Standards

# Security - 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)

## Security- 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.

## Security – Email

- ▶ 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.

# Security -Email attachments

## **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.



# Security-Email Encryption 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

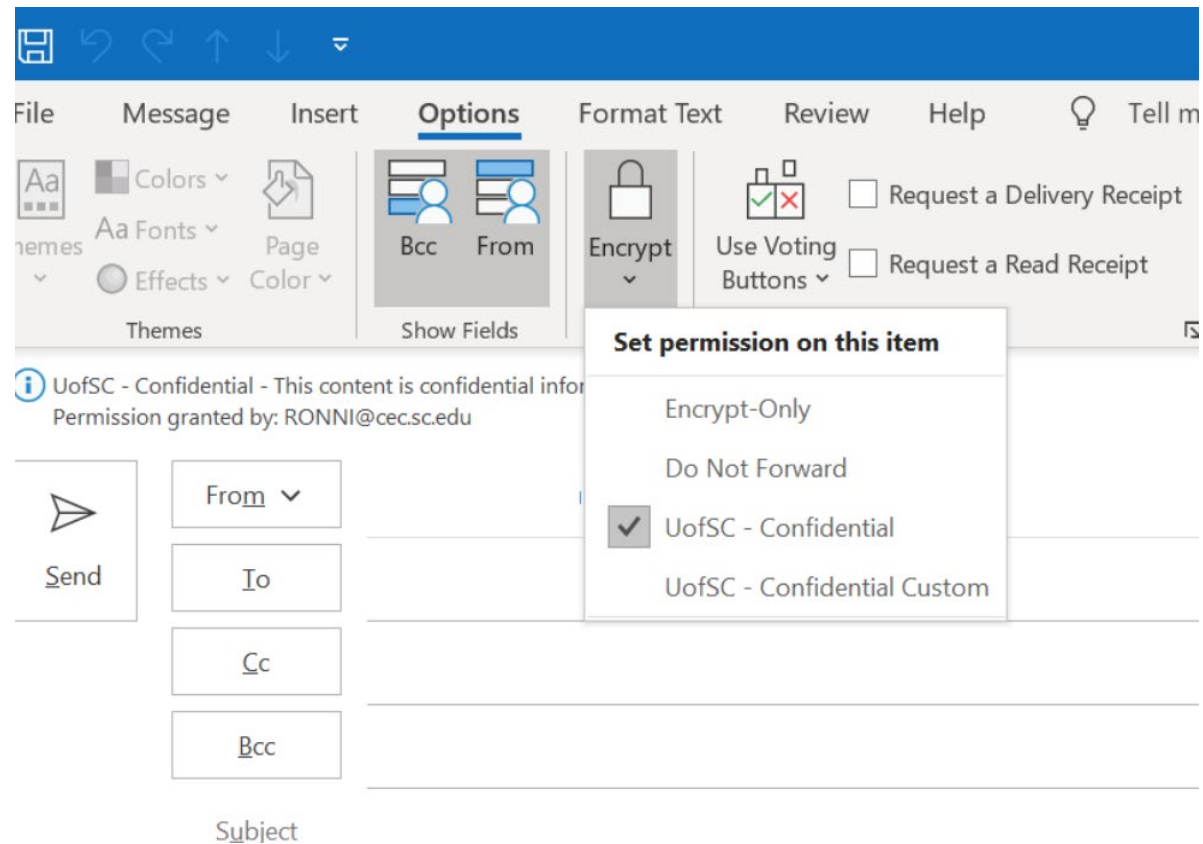
# Security- How to encrypt email in Office 365

- ▶ To send email using USC's email solution to other people using USC email in a more secure environment, you can enable three different mitigations that will help limit the spread of protected communications and data. These mitigations are:
  1. Encryption
  2. Prohibit the use of cut and paste within an email message
  3. Prohibit forwarding of the email address
  4. These can be set both from the Outlook Web browser client and from within the Outlook client with the following procedure.

# Security- How to encrypt email in Office 365

## Instructions

- ▶ Open a new message. Click on the “Options” menu item. You will see and “Encrypt” button in the ribbon. Click it:
- ▶ **To encrypt and prohibit cut and paste**, choose the “UofSC – Confidential” option.
- ▶ **To encrypt, prohibit cut and paste, and prohibit forwarding**, choose the “UofSC – Confidential Custom” option.
- ▶ **NOTE: This only works when sending email to recipients that have accounts in Microsoft’s Office 365 environment.**




# Security- Physical devices

- College of Nursing computer equipment should only be used for authorized purposes in accomplishing your specific duties.
- 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.
- 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.
- Equipment and media can be locked away in a storage area or desk when not in use.
- Unrestricted access to USB ports and removable media devices can facilitate unauthorized copying of data to removable media as well as permit access to removable media which could be infected with malicious software,

# Security- Workstations

A workstation is defined as “an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.”

- Workstations must be positioned 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. To lock your workstation, press Ctrl-Alt-Del or Windows key  + “L”
- Workstation access should be controlled based on job requirements.
- Please check with CON IT before installing any software.
- If devices are lost, stolen or compromised, notify CON IT immediately!

# Security- 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.

# CON AWS Server

INFORMATION

# CON Research AWS Server – R: Drive



Access to the College of Nursing Research AWS server is granted only to authorized individuals with a “need to know.”



Disclosure of PHI via electronic means is strictly forbidden without appropriate authorization.



Do not store data from the AWS server on your desktop, in your OneDrive, or on any device that is not encrypted.



The server is **NOT ACCESSIBLE** off campus unless you use remote desktop to remote into a machine that is physically on campus.



# Access to AWS server

## Onboarding

Faculty who would like to grant server access to grant hires and/or student workers must complete HIPAA training and submit an attestation form before access is granted to the user.

Please place a ticket with the [Nursing Helpdesk in Service Now](#) to request access.

The link to this presentation will be sent to the user.

The attestation form will be sent through Dynamic Forms for the end user to fill out and resubmit.

Once the form is received, the user will be granted access to the folder specified.

## Offboarding

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 an assistant or grant hire 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.



# Data breach

INFORMATION AND PROCEDURES

# 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.

# Incident Response -

- ▶ 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.

## 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 – 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

## 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?

## 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



## 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

## 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**

# 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 by [placing a ticket in Service Now](#). Please provide all pertinent information in your initial ticket.
- ▶ Contact the Nursing Help Desk for any questions or assistance.

**REFERENCES:**

HIPAA COLLABORATIVE  
OF WISCONSIN

USC SCHOOL OF  
MEDICINE

UC BERKLEY | RESEARCH

UNC INFORMATION  
TECHNOLOGY SERVICES

Thanks!

Please complete your training attestation form and return to Nursing TRC staff