Welcome to the HIPAA, Privacy & Security Training Module
Course Competencies

During this course you will learn:

• about the Health Insurance Portability and Accountability (“HIPAA”) Privacy and Security Rules;

• about the HIPAA identifiers that create protected health information (“PHI”);

• how to recognize situations in which confidential and protected health information can be mishandled;

• about practical ways to protect the privacy and security of sensitive information, including PHI; and

• that employees will be held responsible if they improperly handle confidential or protected health information.

This training module addresses the essential elements of maintaining the privacy and security of sensitive information and protected health information (PHI) within the University workplace.
Forms of Sensitive Information

Sensitive Information exists in various forms…

It is the responsibility of every employee to
protect the privacy and security of sensitive information
in ALL forms.
Examples of Sensitive Information

- Social Security numbers
- credit card numbers
- driver’s license numbers
- personnel information
- research data
- computer passwords
- Individually identifiable health information

The improper use or disclosure of sensitive information presents the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to students, faculty, staff, patients, and the University. Breaches of information privacy can also result in criminal and civil penalties for both the University and those individuals who improperly access or disclose sensitive information, as well as disciplinary action for responsible UNC employees.

Every University employee must protect the privacy and security of sensitive information.
HIPAA Privacy & Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule (“Final Rule”) implementing HITECH’s statutory amendments to HIPAA. The deadline for compliance is September 23, 2013.

This training module focuses on two primary HIPAA rules, as amended by HITECH:

- Section 1: The HIPAA Privacy Rule
- Section 2: The HIPAA Security Rule

Note: There is also a Transaction Rule that is not covered in this course. Healthcare providers need to be aware that under this Rule, treatment must be accurately billed using the prescribed code sets.
Section 1A

HIPAA Privacy Rule Overview
Covered Entities
Have a Duty to Protect PHI

A “covered entity” is any person or organization that furnishes, bills, or is paid for health care services in the normal course of business. Pursuant to HIPAA, individually identifiable health information collected or created by a covered entity is considered “protected health information,” or PHI. University departments that use or disclose PHI are governed by HIPAA requirements.
PHI defined

**PHI** is generally defined as:

Any information that can be used to identify a patient – whether living or deceased – that relates to the patient’s past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

Employees may access PHI only when necessary to perform their job-related duties.
Any of the following are considered identifiers under HIPAA.

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives
- Full face photographs or images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.
Affinity Health Plan, Inc. discovered and reported to HHS that it had returned leased photocopiers to the leasing agents without first erasing the data contained on the copier hard drives that included PHI. The breach was estimated to have affected 344,579 individuals. Following an investigation, Affinity entered into a settlement agreement with HHS providing for a $1.2 million payment and a corrective action plan.

Copiers: erase all data from hard drives.
Fax: confirm authorization instructions; verify telephone numbers before faxing; when possible, use pre-programmed numbers.
Device: encrypt; enable and use password protection.
A court ordered Walgreens to pay $1.44 million to a customer whose PHI was impermissibly accessed and disclosed by a pharmacy employee. The employee suspected her husband’s ex-girlfriend gave him an STD, looked up the ex-girlfriend’s medical records to confirm her suspicion, and shared the information with her husband. He then texted his ex-girlfriend and informed her that he knew about her STD.

Multiple state courts have ruled that HIPAA establishes a standard of care to which healthcare provider offices need to adhere, and liability for negligence may arise when that standard of care is breached.
Access Must be Authorized

An employee may only access or disclose a patient’s PHI when this access is part of the employee’s job duties.

Except in very limited circumstances, if an employee accesses or discloses PHI without a patient’s written authorization or without a job-related reason for doing so, the employee violates University policy and HIPAA.
Unauthorized Access

It is never acceptable for an employee to look at PHI “just out of curiosity,” even if no harm is intended (i.e., retrieving an address to send a ‘get well’ card).

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

These rules apply to all employees, including health care professionals.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage, unless the access is required for the individual to do his job. Such improper behavior will be considered by the University when determining disciplinary action against violators.
A breach occurs when information that, by law, must be protected is:

- lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for);
- “hacked” into by people or mechanized programs that are not authorized to have access (e.g. the system in which the information is located is compromised through a “worm”), or
- communicated or sent to others who have no official need to receive it (e.g. gossip about information learned from a medical record).
Facing the most severe level of HIPAA’s criminal provisions – up to 10 years in prison and a $250,000 fine – because the violations involved access and use of PHI for personal gain, an employee of the Seattle Cancer Care Alliance agreed to plead guilty and serve a 16 month prison sentence and pay back both the impacted credit card companies and the patient from whom he stole PHI. The employee accessed and used the patient’s name, birth date, and Social Security number from the medical record to fraudulently obtain four credit cards. He then charged about $9,000 in the patient’s name.

Individual employees, and not just the “covered entities” for whom they work, are subject to HIPAA’s sanctions.
Employees Must Report Breaches

Part of your responsibility as a University employee is to report privacy or security breaches involving PHI to your supervisor AND one of the following persons:

- your HIPAA Privacy Liaison*;
- your Information Security Liaison;
- the HIPAA Privacy Officer;
- the HIPAA Security Officer;
- the Information Security Office, or
- the Office of University Counsel.

Employees, volunteers, students, or contractors of the University may not threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint, including notifying of a privacy or security breach.

Reports of possible information privacy violations can be made through the University’s Compliance Line at http://www.unc.edu/depts/legal/faq.html#

Reports may also be made via telephone by calling the Compliance Line toll-free at 866-294-8688, 24 hours a day, 365 days a year.

* For a list of University HIPAA contact persons, please see UNC-CH HIPAA Contacts
Penalties for Breaches

Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by the University, such breaches may result in civil and criminal penalties.

Statutory and regulatory penalties for breaches may include:

**Civil Penalties:** $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year

**Criminal Penalties:** $50,000 to $250,000 in fines and up to 10 years in prison

The University is required by the North Carolina Identity Theft Protection Act to notify potentially affected individuals of information breaches involving their Social Security numbers and other identifying information. HIPAA requires that the University notify individuals of any breaches involving their unsecured PHI.
Breach Notification Requirements

Any impermissible use or disclosure that compromises PHI or other sensitive information may trigger breach notification requirements. Depending upon the results of a risk analysis of the impermissible use or disclosure, breach notification may have to be made to:

- the Department of Health and Human Services,
- the North Carolina Attorney General,
- all individuals whose information was breached or disclosed, and
- the media.

Letters of explanation describing the circumstances, including responsible parties, may have to be sent. A breach can significantly impact both the economic and human resources of the University. The estimated average cost per compromised record in a data breach can exceed $200. A breach has great potential to harm the reputation of the University, as well.
Massachusetts Eye and Ear Infirmary agreed to pay HHS $1.5 million and retain a independent monitor for HIPAA violations resulting from the theft of an unencrypted laptop containing PHI of patients and research subjects. HHS’s investigation determined that the Infirmary failed to take necessary steps to ensure the confidentiality and security of PHI created, maintained, and transmitted using portable devices.

UNC community members **must report** the loss or theft of any personal or University-owned device as an Information Security Incident to Information Technology Services (ITS) at 919-962-HELP and submit a “critical” remedy ticket.

Refer to the Information Security Policies and Responsibilities at https://help.unc.edu/CCM3_020433
Quick Review

• Sensitive information exists in many forms: printed, spoken, and electronic.

• Sensitive information includes Social Security numbers, credit card numbers, driver’s license numbers, personnel information, computer passwords, and PHI.

• There are a number of state and federal laws that impose privacy and security requirements, including the North Carolina Identity Theft Protection Act and HIPAA.

• Two primary HIPAA regulations are the Privacy Rule and the Security Rule.

• When used to identify a patient and when combined with health information, HIPAA identifiers create PHI.

• An employee must have a patient’s written authorization or a job-related reason for accessing or disclosing patient information.

• Breaches of information privacy and security may result in both civil and criminal penalties, as well as University sanctions. Employees must report such breaches.
Section 1B

HIPAA Privacy Rule

Program Components
Five HIPAA Program Components

Following is a brief overview of five HIPAA program components followed by University covered entities:

1. Individual (Patient) Rights

2. “Minimum Necessary” Information Standard

3. Procedures for Data Use in Research

4. Limits for Marketing and Fundraising Uses

5. Business Associates
1. Patient Rights

HIPAA sets forth the following individual rights for patients.

- To receive a copy of the University’s Notice of Privacy Practices.
- To request restrictions* and confidential communications of their PHI;
- To inspect and/or receive an electronic copy of their healthcare records.
- To request corrections of their healthcare records.
- To obtain an accounting of disclosures (i.e., a list showing when and with whom their information has been shared).
- To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected.
- To receive notice of a breach of their unsecured PHI.

* The Final Rule requires that a covered entity must agree to a request to restrict the disclosure of PHI to his/her health plan for a health care item or service for which the patient has paid in full out of pocket, unless otherwise required by law.
2. Minimum Necessary

Generally, a patient’s authorization is required for the use or disclosure of PHI. When a use or disclosure of PHI is permitted, via patient authorization or otherwise, HIPAA requires that only the amount of PHI that is the **MINIMUM NECESSARY** to accomplish the intended purpose be used or disclosed.
Disclosures of PHI

HIPAA regulations **permit** use or disclosure of PHI for:

- providing medical treatment
- processing healthcare payments
- conducting healthcare business operations
- public health purposes as required by law

Employees **may not** otherwise access or disclose PHI **unless**:

- the patient has given written permission
- it is within the scope of an employee’s job duties
- proper procedures are followed for using data in research
- required or permitted by law

**Note:** the Final Rule now protects the PHI of a **deceased individual** for period of **50 years following the death** of that individual.
Imagine that you work with patients to help find ways to pay their medical bills. Through your work, you become aware of a family under substantial financial hardship. You believe that kindhearted members of the community would provide help “If they only knew” of these circumstances. In order to tell this story you must get specific written authorization from the patients or their legal representatives that identifies whom you will tell. In addition, you may communicate only the minimum amount of information necessary to describe the need.

Note: This type of “outreach” needs to be approved in advance by departmental managers and supervisors and must be consistent with institutional policy.
3. Research Data

HIPAA regulates how PHI may be obtained and used for research. This is true whether the PHI is completely identifiable or partially “de-identified” in a limited data set.

A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation, including an individual patient authorization or an institutionally approved waiver of authorization.

HIPAA requirements for accessing and using PHI in research are explained in the University’s HIPAA and Research page.
Even if a researcher gets a signed “Informed Consent Form” from a research subject, if she does not also get a signed HIPAA Authorization form (or obtain a waiver of authorization from the Institutional Review Board), she may not use data she has collected for her research, presentations or publications.
4. Marketing & Fundraising

- Without first obtaining a patient authorization, the University may not receive payment for the use or disclosure of PHI, nor may the University sell PHI.

- The University may only use demographic information, including name, address, other contact information, age, gender, and date of birth, as well as certain other information about the medical treatment of an individual for fundraising purposes.

- The Notice of Privacy Practices must advise patients of the prohibitions on marketing and the sale of PHI and of their right to “opt out” of being contacted for fundraising purposes.

- Each fundraising solicitation must contain an easy means for patients to “opt out” of receiving such communications in the future.
5. Business Associates

An outside company or individual is a Business Associate of the University when performing functions or providing services involving the use or disclosure of PHI maintained by the University.

Under the Final Rule, a Business Associate is 

directly liable for compliance

with HIPAA Privacy and Security requirements and must:

• enter into a Business Associate Agreement (called a BAA) with the covered entity (the University);
• use appropriate safeguards to prevent the access, use or disclosure of PHI other than as permitted by the contract, or BAA, with the covered entity;
• obtain satisfactory assurances from any subcontractor that appropriate safeguards are in place to prevent the access, use or disclosure of PHI entrusted to it;
• notify the covered entity of any breach of unsecured PHI for which the Business Associate was responsible upon discovery;
• ensure its employees and/or those of its subcontractors receive HIPAA training; and
• protect PHI to the same degree as a covered entity.
Quick Review

Under HIPAA, patients have the right to:

• receive a copy of the University’s *Notice of Privacy Practices*

• receive a copy of their healthcare records in electronic form

• ask for corrections to their healthcare records

• receive an *accounting* of when and to whom their PHI has been shared

• restrict how their PHI is used and shared

• authorize *confidential communications* of their PHI to others

• receive notice of a breach of their unsecured PHI

• file a HIPAA *complaint*
Quick Review

• The University may use or share only the **minimum necessary information** to perform its duties.

• Patients must sign an **authorization form** before the University can release their PHI to a third party not involved in providing healthcare.

• A researcher or healthcare provider is not entitled to use PHI in research without the appropriate **HIPAA authorization** or a waiver of authorization.

• The University must obtain an individual’s **specific authorization** before using his or her PHI for the **sale of PHI, marketing, and some fundraising efforts**.

• A contractor providing services involving PHI is called a **Business Associate**.

• A covered entity and business associate must enter into a **Business Associate Agreement (“BAA”)**.

• Business Associates are directly liable for HIPAA compliance and must ensure that their **employees or subcontractors receive HIPAA training** and employ appropriate safeguards for PHI.

• HIPAA protections apply to a **deceased person’s PHI for 50 years** after they have died.
Section 2

HIPAA Security Rule
HIPAA Security Rule

The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the **confidentiality, integrity, and availability** of PHI.

**Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.

**Integrity** means that data or information has not been altered or destroyed in an unauthorized manner.

**Availability** means that data or information is accessible and useable upon demand only by an authorized person.
Security Standards/Safeguards

The University is required to have administrative, technical, and physical safeguards to protect the privacy of PHI.

Safeguards must:

- Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others) and work areas;

- Limit accidental disclosures (such as discussions in waiting rooms and hallways); and

- Include practices such as encryption, document shredding, locking doors and file storage areas, and use of passwords and codes for access.
Irritated by a patient who was always late to her prenatal appointments, a Missouri doctor posted to her personal Facebook page, “may I show up late to her delivery?” A reader took a screen shot of the doctor’s comment and posted it to the employing hospital’s Facebook page for expectant mothers where many wrote to demand the doctor’s termination.

The doctor’s post revealed the patient’s induction date and that she had previously suffered a stillbirth making identification likely. The employing hospital publicly issued a comment decrying the incident.

University employees should never disclose work-related sensitive information through social media such as Facebook, Twitter, and Google+.
Viruses, worms, spyware, and spam are examples of malicious software, sometimes known as “malware”.

Employees should utilize antivirus and anti-spyware software, and update it regularly with patches (links can be found through UNC Shareware Distribution at https://shareware.unc.edu/links.html).

Safe Internet browsing habits can also reduce the likelihood of an infection; do not open email or click on embedded links from an unknown or untrusted site.

If the computer or mobile device you are using stores work-related sensitive information, personal use of the web is not recommended.
Viruses

Another major threat to the University’s information system and to your data is computer viruses.

- Viruses “infect” your computer by modifying how it operates and, in many cases, destroying data.
- Viruses spread to other machines by the actions of users, such as opening infected email attachments.
- Viruses can forward PHI to unauthorized persons by attaching themselves to documents, which are then emailed by the virus.
- Newer viruses have their own email engines, enabling them to send email without having to use an email client or server.
- Many viruses also install a “backdoor” on affected computer systems allowing for unauthorized access and collection of Sensitive Information.
Worms

Worms are programs that can:

• run independently without user action;
• spread complete working versions of themselves onto other computers on a network within seconds; and
• quickly overwhelm computer resources with the potential for data destruction as well as unauthorized disclosure of sensitive information.
Spyware

Spyware is software that is secretly loaded onto your computer, monitors your activities, and shares that information without your knowledge.

Malicious websites can install spyware on every computer that visits those sites.
Spam and Phishing

**Spam** is an unsolicited or “junk” electronic mail message, regardless of content.

**Spam** usually takes the form of bulk advertising and may contain viruses, spyware, inappropriate material, or “scams.”

**Spam** also clogs email systems.

**Phishing** is a particularly dangerous form of spam that seeks to trick users into revealing sensitive information, such as passwords.

**REMEMBER:** University ITS will never ask you to disclose passwords, social security numbers, or other sensitive information via email.

For example, in August of 2013, an unauthorized website sent email to UNC users as “Carolina Connect 2.0” and asked users to login with their ONYEN and password. ITS sent an email the following day reminding all users: NEVER provide ONYEN credentials to an unauthorized third party. Uncertain? DON’T respond! Call 919-962-HELP or email ITS Security, security@unc.edu.
“Trendjacking” is a recent phishing scam that is particularly dangerous. Emails come from what looks like CNN or other news sources and include current news stories, the latest celebrity scandal, medication ads, etc. They also contain dangerous links which, once clicked on by the email recipient, direct the recipient’s web browser to a website that contains a multiple vector attack that throws every known hack at the recipient’s computer looking for unpatched software that can be exploited. Once exploited, a virus or malware is installed on the recipient’s computer or device and any information that recipient accesses is at risk.

When the recipient of that “trendjacking” email uses his/her computer or device to access PHI or other sensitive information that information is then exposed to risk. Such exposure could result in illegal use of the information obtained.

Theft of health records has become big business and is on the rise. Identify theft of health records costs the United States more than $40 billion and affected 1.85 million people just in 2012 alone!

The best protection? Be skeptical about emails!
Safe Browsing Habits

• **Safeguard sensitive information**
  Look for signs of security when providing sensitive information (i.e. the web address starts with “https” or a padlock icon is displayed in the status bar).

• **Keep browser updated and use security settings**
  • Stay current with browser updates and application updates such as Adobe Flash and Acrobat.
  • Enable browsing security settings to alert you to threats to your computer like popups, spyware, and malicious cookies.

• **Use security software**
  There are a number of free and easily available software products to protect your computer from malware, spyware, and virus threats. Talk to your IT support personnel to find out which software best fits your needs.

• **Safe downloading & streaming**
  • When in doubt just don’t do it! If a download looks too good to be true, it might be malware.
  • Downloaded files like software or other media can contain hidden malware.
  • Streaming media Web sites might seem harmless, but watching or listening to streaming media may require downloading a special media player that may contain malware.
Peer to Peer (P2P)  
File Sharing Programs

Use of P2P programs on University networks is **prohibited** in certain areas, especially those where PHI is present.

Check with your HIPAA Privacy or HIPAA Security Officer before using P2P programs.

- **P2P** programs frequently contain spyware and are used to share files that contain malware.

- **P2P** file sharing programs such as Shareaza, Ares, Limeware, Kazaa, BearShare, eMule, and BitTorrent are used to download unauthorized or illegal copies of copyrighted materials such as music or movies. They may also expose Sensitive Information to unauthorized individuals if not configured correctly.
Safe Computing and Email Use

- University policy requires that written approval be granted by a Dean or Department Head before storing PHI or PII on mobile devices.
- Encryption is required when a University employee sends or receives PHI or PII to a destination address outside the campus network.
  
  For further information, contact your unit’s Security Officer or IT support person, or contact the ITS help desk at 962-HELP.

- When traveling, working from home, or using a mobile device, a University employee whose work involves the transmission of PHI or PII must encrypt the data UNLESS the employee uses a VPN connection AND transmits data only to a destination within the campus network.

- Do not open email attachments if the message looks the least bit suspicious, even if you recognize the sender. “When in doubt, throw it out.”

- Do not respond to “spam” – simply discard or delete it, even if it has an “unsubscribe” feature.

For more information regarding the University’s policies governing the transmission of PHI and PII over wireless networks visit:
Mobile Devices

University policy requires written approval from a Dean or Department Head in order to store Sensitive Information, including PHI, on mobile devices. This applies to all mobile computing devices such as laptop PCs, PDAs such as iPads, smart phones or even regular cell phones.

Employees must utilize the following security controls when storing and transmitting sensitive information:

- strong power-on passwords
- automatic log-off
- display screen lock at regular intervals while the device is inactive
- encryption

Never leave mobile computing devices unattended in unsecured areas.

Immediately report the loss or theft of any mobile computing device to your supervisor and the Information Security Office.

Remember, for any mobile device, encryption is the best defense!
Password Control

Many security breaches come from within an organization and many of these occur because of bad password habits.

- **Use strong passwords** where possible (at least 8 characters, containing a combination of letters, numbers, and special characters).

- **Change your passwords frequently** (45-90 days) to prevent hackers from using automated tools to guess your password.

- **It is a violation of University Policy to share your password with anyone.** Electronic audit records track information based on activity associated with user IDs.
Password Management

With the growing trend for web sites and services to require visitors to create new user IDs and passwords to access the site, people are finding it difficult to safely manage a large number of accounts. One solution is to use a “password vault,” which provides an easy method to store all of one’s passwords in an encrypted format.

Two password vaults that have been used at UNC include:
- Keepass (http://keepass.info/)
- Roboform (www.roboform.com).
A health clinic employee set his phone to “auto-forward” his University messages to his Google account, despite it being against University policy. His supervisor sometimes sent assignments to his Google email address, as well. His phone was not password protected.

While on vacation, the employee’s phone “went missing”. Eventually the phone was returned by a travel office, but no one knows who may have had possession of the device while it was not in the employee’s control.

The employee violated HIPAA by storing and transmitting PHI to an unsecure device, creating a risk of breach that could require notification to each affected client/patient whose data was contained in the phone and possibly the government. There will also be disciplinary implications for the employee and his supervisor.

Costs to the University of a lost or stolen mobile device go far beyond the cost of replacing the device itself. The majority of expenses include:

- investigative costs
- reporting data breaches
- liability for data breaches (e.g. government penalties)
- restoring hard-to-replace information
- preventing further misuse of the data
- lost intellectual property
- lost productivity
- damage to reputation

A recent study found that laptop loss led to losses of $2.1 billion for the 329 organizations surveyed during a one year period. Cleaning up the resulting data breaches accounted for 80% of that total.

According to a 2013 Ponemon Institute report:
- 41% of breaches are due to malicious/criminal attacks
- 29% are due to a system glitch
- 33% are due to the “human factor”

Report any missing, lost, or stolen device immediately!
Remote Access

All computers and mobile devices used to connect to University networks or systems from home or other off-site locations should meet the same minimum security standards that apply to your work computer.

You should:

- Make use of the Virtual Private Network (VPN) at home or off-site, AND transmit PHI or PII only to locations within the campus network. Otherwise, sensitive data must be encrypted.

- Run Windows Update or the update feature of the particular operating system that you are using. Don’t forget to also update your applications (e.g. QuickTime, RealPlayer, and your preferred web browser)!

- Keep virus definitions current by using the antivirus software recommended and supported by ITS, currently Microsoft System Center Endpoint Protection for university-owned computers. For personal computers, the University recommends Microsoft Security Essentials for Windows Operating System and Clam X Antivirus for Mac Operating System.

**DO NOT** let your antivirus subscription expire!

Faculty and Staff may obtain antivirus software via the University’s site license through [https://shareware.unc.edu/](https://shareware.unc.edu/).
A University of Rochester Medical Center physician misplaced an unencrypted USB drive containing PHI of 537 patients, including demographic identifiers as well as diagnostic information. Because of this negligence, the Medical Center must notify all of the individuals affected by this breach, the attorney general, and HHS, triggering the possibility of further investigation and large fines.

Whenever possible, avoid using external storage devices to store Sensitive Information. If you must use such devices, including “thumb” or “flash” drives, use encryption, and adhere to the following:

- Use portable storage media only for transporting information, and not to permanently store information.
- Once you’ve used the information, erase it from the device.
- Consider attaching your memory stick to your key ring -- you are less likely to lose your keys.
Employee Responsibilities

- Avoid storing sensitive information on mobile devices and portable media, but if you must, you must use **encryption**.
- Always keep portable devices physically secure to prevent theft and unauthorized access.
- Access information only as necessary for your authorized job responsibilities.
- Keep your passwords confidential.
- Comply with the University’s Information Security and Privacy policies.*
- Report promptly to your supervisor and the University’s HIPAA Privacy or Security Officer the loss or misuse of devices storing PHI or other Sensitive Information.

*see [HIPAA Privacy Policy](#) and [UNC Information Security Policies](#)
Communications in Public Areas

Be aware of your surroundings when discussing Sensitive Information, including PHI. Do not discuss Sensitive Information or PHI in public areas such as in cafeterias or restaurants, while walking on campus, or while riding the bus.

Use caution when conducting conversations in:
- semi-private rooms
- waiting rooms
- corridors
- elevators and stairwells
- open treatment areas.
Appropriate Disposal of Data

Observe the following procedures for the appropriate disposal of Sensitive Information, including PHI.

- Hard copy materials such as paper or microfiche must be properly shredded or placed in a secured bin for shredding later.
- Magnetic media such as diskettes, tapes, or hard drives must be physically destroyed or “wiped” using approved software and procedures. Contact the Information Security Office or consult the UNC-Chapel Hill Campus Standards for Electronic Media Disposal for more information.
- CD ROM disks must be rendered unreadable by shredding, defacing the recording surface, or breaking.

Sensitive information and PHI should never be placed in the regular trash!
On several occasions sensitive materials have been left in file cabinets or office desks that have been turned in to the UNC Surplus department. The surplus staff found the sensitive materials and returned them to the Research Compliance Office before anyone picked up the furniture. If any of that furniture had been sold to the public before the sensitive materials were found, it would’ve been difficult and costly for the University to retrieve the materials and manage the breach.

One can’t be too careful when disposing of desks, file cabinets and other office furniture that may hold documents in them. Please check them carefully and confirm that all documents have been removed and properly disposed of before sending furniture to the UNC Surplus department.
Physical Security

- Computer screens, copiers, and fax machines must be placed so that they cannot be accessed or viewed by unauthorized individuals.
- Computers must use password-protected screen savers.
- PCs that are used in open areas must be protected against theft or unauthorized access.
- Servers and mainframes must be in a secure area where physical access is controlled.
What if there is a breach of confidentiality?

Breaches of the University’s policies or an individual’s confidentiality must be reported to the employee’s supervisor AND one of the following persons:

- your HIPAA Privacy Liaison;
- your Information Security Liaison;
- the HIPAA Privacy Officer;
- the HIPAA Security Officer;
- the Information Security Office, or
- the Office of University Counsel.

The University is required to take reasonable steps to lessen harmful effects of a confirmed breach involving compromised PHI. This includes notifying individuals whose information has been breached. The University must report breaches both to the Secretary of Health and Human Services and to the state at least once a year.
Individuals who violate the University’s Information Security Policy* will be subject to appropriate disciplinary action as outlined in the University’s personnel policies, as well as subject to possible criminal or civil penalties.

*see UNC Information Security Policies
Best Practice Reminders

- **DO** keep computer sign-on codes and passwords secret, and **DO NOT** allow unauthorized persons access to your computer. Also, use locked screensavers for added privacy.
- **DO** keep notes, files, memory sticks, and computers in a secure place, and be careful **NOT** to leave them in open areas outside your workplace, such as a library, cafeteria, or airport.
- **DO NOT** place PHI or PII on a mobile device without required approval. **DO** use encryption when sending or storing PHI or PII on mobile devices, including “thumb” or “flash” drives.
- **DO** hold discussions of PHI in private areas and for job-related reasons only. Also, be aware of places where others might overhear conversations, such as in reception areas.
- **DO** make certain when mailing documents that no sensitive information is shown on postcards or through envelope windows, and that envelopes are closed securely.
- **DO NOT** use unsealed campus mail envelopes when sending sensitive information to another employee.
- **DO** follow procedures for the proper disposal of sensitive information, such as shredding documents or using locked recycling drop boxes.
- When sending an e-mail, **DO NOT** include PHI or other sensitive information such as Social Security numbers, unless you have the proper written approval to store the information and use encryption.
HIPAA Web Resources

UNC HIPAA Page

UNC HIPAA Contact Persons

UNC HIPAA Forms and Policies

UNC HIPAA Resources for Researchers

UNC ITS Information Security Policies

U.S. Dept. of Health & Human Services HIPAA Page