Confidentiality, Privacy, and Information Security

Click on the button below to go through the slides in the course.
Instructions for This Online Course

• Move through the slides by clicking the Next button at the lower right of the screen.

• Answer all questions as they occur and click the Submit button. You must get the answer correct before you will be permitted to continue through the course.
Privacy and Information Security are key elements of the UNC Health Care System Compliance Program.

No matter where you are located within the UNC Health Care System every employee is responsible for understanding and following all privacy and security policies.
Objectives

When you complete this course, you will be able to:

• Identify types of confidential information.
• Describe best practices for safeguarding information in spoken, written or electronic formats.
• Understand your responsibility for data encryption
• Describe your responsibilities for protecting information and reporting violations.
• Identify consequences for violations.
• Locate your affiliate’s Privacy, Information Security and/or Compliance Offices.
Every UNC Health Care employee is responsible for protecting confidential information.

There are different types of confidential information at UNC Health Care:
Information About Patients
(Protected Health Information (PHI))

Identifiable Patient Information
Unique identifiers including:

• Name
• Address
• dates of birth, admission, discharge, death
• telephone and fax numbers,
• email address
• medical record number
• health plan beneficiary number
• Social Security number
• account number
• certificate/license number
• any vehicle or other device serial number
• web URL
• Internet Protocol (IP) address
• finger or voice prints,
• photographic images
• Medical history & treatment
• Financial information (insurance, credit/debit card numbers)

Information About Employees

Employee Information

• Driver’s license number
• Social Security number
• Bank account numbers
• User ID and passwords

Information About UNC Health Care

UNC Health Care Information

• Financial and operational information
• Trade secrets of vendors and research sponsors
• System access passwords
There are 2 things to remember about protecting confidential information:

Access information only if you need it to do your job.

Share information only with others who need it to do their jobs.
Test Your Knowledge

Which of the following is NOT confidential?

A) Patient or employee Social Security numbers
B) Patient age and weight
C) Hospital address
D) Organization financial data
E) Passwords
F) Plan of care
G) Clinical test results
H) Patient insurance information
I) Medical history
Confidential information is stored and shared in the following ways:

- **Verbal Communication** *(talking)*
- **Paper Documents**
- **Electronic Data**
Verbal Communication

When talking about confidential information make sure you are:

Sharing only with someone who needs to know the information to perform their job.

Speaking where others (including patient family members and friends) cannot hear, if possible.

Giving only the minimum amount of information necessary.
Verbal Communication

When talking about confidential information be aware of your surroundings!

Avoid discussing PHI in public areas such as cafeterias or elevators, etc.

When conversations in open areas cannot be avoided, remember to keep your voice low.
What Would You Do?

You walk into a patient room to discuss the patient’s care. The patient has a sensitive diagnosis (such as HIV or substance abuse). The patient has two visitors with her and they are having a calm, friendly conversation.

You: *(click on one of the options below)*

A) Ask the patient if it is okay to speak about their care with others present.

B) Ask the visitors to leave the room before speaking to the patient.
Your facility’s Health Information Management (HIM) Department is primarily responsible for releasing (or making available) PHI, but sometimes personnel in other departments release PHI.

- Nursing Services and other support departments may release a copy of the medical record to health care personnel transporting the patient to another health care facility.
- Physicians and nurses may release some information to the patient.
- Physicians and staff who have received the appropriate training may also release to the patient a Patient Clinical Summary (also known as an After Visit Summary at the UNC PN Clinics).

*Call your HIM Department with questions about releasing PHI.*
Your Medical Record
To access your own medical record, complete an authorization form and submit to the HIM Department.

The HIM Department will notify you when you are approved to view your medical record.

PHI for Research
Researchers that request PHI for research must submit appropriate documentation.

See the UNC Research Web Page (http://www.med.unc.edu/www/research) for specific procedures.

Accounting for Disclosures
If your department releases PHI outside of the UNC Health Care System for reasons other than treatment, payment or health care operations, you may need to track those disclosures.

- Use the Disclosure Trac System
- Refer to the Accounting of Disclosures Policy (http://intranet.unchcare.org/policies/unc-hcs-policies-pdf-new-format/ADMIN0051%20pdf.pdf) for specific requirements.

Call your HIM Department with questions about releasing PHI.
What Would You Do?

You have completed the authorization form and turned it into the HIM Department.

Can you view your records now?
(click on one of the options below)

- A) Yes
- B) No
Tips for Releasing PHI

• Review information before sending to make sure you are only sending what is necessary.

• Double-check the e-mail address or fax number. Faxing information to the wrong number may lead to disciplinary action.

• Fax only when mail delivery is not fast enough to meet the patient’s needs.

• Always use a fax cover sheet with Confidentiality Notice (available on the HR Intranet under Forms).

• Email scanned documents to yourself before e-mailing them to the final recipient.
Here’s a test to determine if you can use or share PHI

Ask:

1. Is the disclosure for treatment, payment or health operations purposes?
2. If not, do you have written authorization from the patient?
3. If not, is there another legal requirement for disclosure?

If the answer is “No” to all 3, do not access, use or share the PHI.
Disposal of Confidential Information

Never place confidential information in the trash!

Cross-cut shred or place in secure disposal bins:

- paper
- microfiche
- CD-ROMs
- diskettes
Disposal of Confidential Information

Electronic and Leased Equipment

Computer hard drives must be physically destroyed or “electronically shredded.” Contact your Information Services department for assistance.

Some leased equipment has ability to store information, e.g., copiers. When leased equipment is returned to vendor be sure all confidential information has been removed.
What Would You Do?

You need to dispose of paper or electronic materials that contain protected information.

You:

Option 1: Place in a secured bin.
Option 2: Call your Help Desk and ask them to destroy your hard drive.
Option 3: Mark out the identifying information and throw it in the trash.

A) Only option 1.
B) Options 1 and 2.
C) Any of the above.
B) Options 1 and 2.
C) Any of the above.
A subpoena is a document issued by a court that requires a person to appear in court or to give some kind of evidence. If you receive a subpoena, it is critical to alert the right department.

For billing document requests, direct the person presenting the subpoena to the Billing Department.

For medical record requests, direct the presenter to the Health Information Management Department.

For all other subpoenas, direct the presenter to the Legal Department. (If your affiliate does not have a legal department, contact your Compliance Office).

A subpoena does not remove HIPAA privacy protections. An authorization signed by the patient or a court order signed by a judge is required for releasing confidential information. Contact the Legal Department for guidance before responding to a subpoena.
For all other subpoenas, direct the presenter to the **Legal Department**. *(If your affiliate does not have a legal department, contact your Compliance Office).*

A subpoena does not remove HIPAA privacy protections. An authorization signed by the patient or a court order signed by a judge is required for releasing confidential information. Contact the Legal Department for guidance before responding to a subpoena.
What Would You Do?

Your best friend calls and has forgotten the location of her appointment today. She gives you verbal authorization to look up her appointment in another clinic.

You:

A) Look up her appointment information.
B) Refer your friend to the clinic or to Registration.
Verbal authorization is not recognized by the Privacy Rule or the UNC Health Care System.
What Would You Do?

Your neighbor calls and asks if you can get the room number of a mutual friend who they believe has been admitted to the hospital. You:

A) Look up the information yourself and provide the room number to your neighbor.

B) Refer your neighbor to the hospital operator.
Protecting Electronic Data

Confidential information stored on computers and other electronic devices requires special measures to keep it private.

To protect confidential information stored as electronic data, you should:

- Avoid internet threats
- Ensure data is encrypted
- Use social media and blogging sites appropriately
- Create strong passwords
- Secure computers and other mobile devices
Internet Threats!

Phishing is unwanted e-mail ("spam") that tries to trick you into revealing confidential information, like passwords or credit card information.

Do not reply to any e-mail message that might be a phishing attempt. Call the sender if in doubt.

When it comes to the Internet, if you are not sure it is safe, do not click on links or download files.

Text Captions

Internet Threats!

Phishing

Phishing is unwanted e-mail ("spam") that tries to trick you into revealing confidential information, like passwords or credit card information.

Do not reply to any e-mail message that might be a phishing attempt. Call the sender if in doubt.
Malware

Malware is software (computer programs) designed to harm your computer. Types of malware include viruses, worms and spyware. Malware can destroy your data and expose confidential information.

Malware gets into your computer through e-mail attachments, compromised websites, holes in software and other ways.

The best way to block malware is to always use an up-to-date antivirus program and an antispyware scanning program. Contact your Help Desk for assistance.

Cloud Computing

“Cloud” Computing lets you access computer files and programs over the Internet. Gmail, Google Calendar, Google Docs, Dropbox, Yahoo, etc. are cloud services.

NEVER store confidential information on public cloud services.

Some cloud services advertise HIPAA compliance. These sites cannot be used unless they have a Business Associates Agreement in place with UNC Health Care System.

Personal E-mail

Do not use personal e-mail accounts to conduct UNC Health Care System business or to send confidential information.

Your personal e-mail account is often less secure than your work issued account, so limit access from UNC Health Care System computers.

UNC and UNC Health Care System policy prohibits auto-forwarding of UNC Health Care System e-mail to a personal e-mail account.

When it comes to the Internet, if you are not sure it is safe, do not click on links or download files.
Potential Phishing Message

When it comes to the Internet, if you are not sure it is safe, do not click on links or download files. If you have any questions contact your Affiliate’s Help Desk.
Encryption

What is Encryption?
Encryption makes electronic data (on computers and mobile devices, such as laptops and smart phones) unreadable. Only authorized users of the data will have a key to “unlock” the encryption.

Encryption Requirements
Any confidential information that is sent electronically must be encrypted.

This includes e-mail and information sent over public wireless networks.
E-mail Encryption
Confidential data should not be emailed outside your health care network. If you have a need to use email for transmitting confidential information, be sure to:

1) obtain approval from your manager or supervisor and
2) protect the contents with encryption.

If you do not know how to protect the contents with encryption, you should refrain from sending confidential information via email. Contact your email administrator or your information security representative for assistance.

Encryption Resources
You are responsible for ensuring that you are using encryption when necessary. If you have any questions, please direct them to your affiliate specific contact listed on the following printable slide.
Encryption Resources

UNC Hospitals, UNC Faculty Physicians, UNC Physicians Network, REX, High Point Regional and Chatham employees

Contact for Encryption guidance:

soc@unch.unc.edu

UNC School of Medicine employees

Contact for Encryption guidance:

ITS Help Desk/919-962-HELP

Caldwell employees

Contact for Encryption guidance:

Help Desk 828-757-5245

Pardee employees

Contact for Encryption guidance:

Help Desk 828-696-1190
Social Media and Blogging

Social media sites (Facebook, Twitter, LinkedIn, Google+, etc.) and blog sites (WordPress, Blogger, LiveJournal, etc.) allow you to easily share information with your friends and the public.

Never post protected health information or confidential information of any kind on social media or blog sites.
What Would You Do?

You log onto Facebook after work and see that a coworker has posted the following update:

*My elderly neighbor came into my clinic today for treatment. Please keep her in your thoughts for a quick recovery.*

You:

- A) Do nothing
- B) Print the update and report it to the Privacy, Security or Compliance Office
- C) Respond to the update or tell the employee that this is a privacy violation and should be removed
C) Respond to the update or tell the employee that this is a privacy violation and should be removed
Test Your Knowledge

Select the inappropriate social media posts and comments below:

A) Susie Smith Glad you had a good day! My “favorite” patient was in the clinic again today and still not comp with his meds! o_O

B) Jimmy Jones John, just sent you a wicked pic of a chest wound we saw in the ED today!

C) Betty Brown We had a local celebrity on the unit! Call me!

D) Joe White Every day in Chapel Hill is a great day!
Passwords

A “strong” password is an important way to protect confidential information stored as electronic data.

Roll over each password below to find out if it is a strong password.

**ladybug1**
This password is weak. Actual words, dates, nicknames and names of family, friends or pets are easily guessed.

**abcde**
Weak. Do not use sequences (12345, qwerty) or repeated characters (22222). Make sure passwords are at least 6 characters long.

**1@dybu9!**
Strong. Mixing numbers, letters and special characters creates a stronger password.

---

Text Captions

**Passwords**

A “strong” password is an important way to protect confidential information stored as electronic data.

**ladybug1**
This password is **weak**. Actual words, dates, nicknames and names of family, friends or pets are easily guessed.

**abcde**
**Weak**. Do not use sequences (12345, qwerty) or repeated characters (22222). Make sure passwords are at least 6 characters long.
1@dybu9!

**Strong.** Mixing numbers, letters and special characters creates a stronger password.
What Would You Do?

You have to pick a new password that is easy to remember, but hard to guess. Which of the following do you choose?

A) Ladybug (your dog’s name)

B) Badgers (your favorite team’s name)

C) Tm2tbg# (based on the phrase “Take me to the ball game.”)
What Would You Do?

A new employee arrives in your work area but does not have a user ID and password yet. Your supervisor instructs you to log the new employee into the system under your user ID and password while you train them.

You:

A) Follow your supervisor’s instructions.

B) Remind your supervisor that you are not allowed to share your password and ask them to call your affiliate’s computer support center to check on the new employee’s user ID and password.
B) Remind your supervisor that you are not allowed to share your password and ask them to call your affiliate’s computer support center to check on the new employee’s user ID and password.
Security for Computers

Turn your screen away from public areas. Position printers and fax machines out of public areas (like waiting rooms).

Log out or lock your computer when you leave. You can quickly lock your computer by pressing the Windows key and the L key at the same time.

Lock your computer
Security for Mobile Devices

Any mobile device with confidential information on it should be encrypted. If not able to be encrypted (e.g., a camera) it should be physically secured when not in use in a locked drawer or safe. Make sure you know where these devices are at all times.

Report any loss or theft of a mobile device containing confidential information to your affiliate’s computer support center immediately.

Some common mobile devices:

- laptops
- tablets
- smart phones
- cell phones
- flash drives
- memory cards
- CDs/DVDs
- external hard drives
- cameras
Some common mobile devices:

- laptops
- tablets
- smart phones
- cell phones
- flash drives
- memory cards
- CDs/DVDs
- external hard drives
- cameras
Actual Privacy and Security Violations

- PowerPoint presentation containing patient PHI for which authorization had not been obtained. The presentation was made to about 80 people.

- Unauthorized access of a patient’s account by a physician who assumed it was okay because they were a “friend of the family.”

- Unauthorized patient PHI used in a publication that was mailed to approximately 16,000 recipients.

- An external hard drive containing patient names, medical record numbers, dates of admission, medications, diagnosis and treatment information was lost or stolen.
• Access of a high profile patient’s account by over 60 employees of all levels.

• A printout containing PHI left on a table in a café.

• Thirty-one medical records lost by a physician and found by a Department of Corrections inmate.

• Disclosure of a very sensitive diagnosis to individuals not authorized.

• Lost and/or stolen smart phones, thumb drives and laptops which were not password protected or encrypted.
Reporting Privacy and Security Violations

Remember, if you are aware of or suspect a violation, you are required to report it to any of the people below:

- Your supervisor
- Privacy Office
- Information Security Office
- Compliance Hotline *(accepts anonymous reports)*

**Supervisors are required to report any suspected violation reported by an employee to the Privacy or Information Security Office.***
Issues that Should Be Reported

- Stolen laptop
- Lost smart phone
- Misplaced patient records
- Lost hospital contract
- Co-workers sharing passwords
- Misdirected faxes and mail
- Human error
- Overheard conversations
- Inappropriate social media posts

Loss of confidential information or equipment containing confidential information

Misuse of information, system access, or sharing of passwords

Accidental or unauthorized disclosures of protected information

Issues that Should Be Reported

Loss of confidential information or equipment containing confidential information

- Stolen laptop
- Lost smart phone
- Misplaced patient records
- Lost hospital contract
Misuse of information, system access, or sharing of passwords
• Co-workers sharing passwords

Accidental or unauthorized disclosures of protected information
• Misdirected faxes and mail
• Human error
• Overheard conversations
• Inappropriate social media posts
Special Reporting Requirements for Social Security Numbers

The confidentiality of Social Security numbers has special legal protection.

If Social Security numbers are released or disclosed to anyone who does not have a need to know them to perform their job, this must be reported immediately to your supervisor, the Privacy Office or the Information Security Office.

The UNC Health Care System is required to take additional steps in a timely manner when Social Security numbers are inappropriately released.
What Would You Do?

I observed something I think could be violation. Even though I am unsure, I trust my instincts and contact:

- A) My supervisor
- B) My affiliate’s compliance hotline
- C) Send an e-mail to Compliance@unch.unc.edu
- D) Any of the above
When in doubt trust yourself! Report any issues of concern. Let the Privacy Office investigate.

Don’t know who to contact?

A printable list of the UNC Health Care System Privacy, Information Security and Compliance Contacts can be found on the next slide.
UNC Health Care System Privacy, Information Security, and Compliance Contacts

**UNC Hospitals, UNC Faculty Physicians, UNC Physicians Network**
- Privacy Office: 919-966-9615
- Privacy Hotline: 919-843-2233
- Compliance Hotline: 800-362-2921
- Information Security Office: 919-966-5647
- Compliance Office: 919-966-8505
- http://intranet.unchealthcare.org/hospitaldepartments/hipaa

**UNC School of Medicine**
- Privacy Office: 919-966-9900
- Privacy Hotline: 919-966-9900
- Compliance Hotline: 919-966-9900
- Information Security Office: 919-966-9900
- Compliance Office: 919-966-9900
- http://www.med.unc.edu/security

**REX**
- Privacy Office: 919-784-3436
- Privacy Hotline: 919-784-7788
- Compliance Hotline: 877-CARE REX (877-227-3739)
- Information Security Office: 919-784-4357
- Compliance Office: 919-784-6552
- www.rexhealth.com/privacy-hipaa-policies
- 877-CARE REX (877-227-3739)
Pardee
Privacy Office: 828-696-4251
Privacy Hotline: 828-696-4701
Compliance Hotline: 828-696-4701*

Hotline change in 2014 - If number not working
call Compliance Hotline for UNC Hospitals

Information Security Office: 828-696-4251
Compliance Office: 828-696-4251
http://supportcenter/doccenter/Departmental%20Processes/Forms/AllItems.aspx

High Point Regional
Privacy Office: 336-878-6550
Privacy Hotline: 800-826-6762
Compliance Hotline: 800-826-6762

Information Security Office: 336-878-6570
Compliance Office: 336-878-6970
No Web Site at this time

Chatham Hospital
Privacy Office: 919-799-4004
Privacy Hotline: 919-843-2233
Compliance Hotline: 800-273-8452

Information Security Office: 919-799-4004
Compliance Office: 919-799-4004
http://intranet.unchartedcare.org/hospitaldepartments/hipaa

Caldwell
Privacy Office: 828-757-5177
Privacy Hotline: 828-757-5555
Compliance Hotline: 828-757-5555

Information Security Office: 828-757-5555
Compliance Office: 828-757-5555
No Web Site at this time
Consequences for Violations

• UNC Health Care disciplinary action up to and including termination.

• Fines range: $100 - $50,000 per violation. One incident could result in numerous violations and therefore multi-million dollar fines.

• Jail time: 1-10 years

Failure to report a violation is a violation!
Confidentiality Statement

Click [here](http://unchealthcare.org/site/humanresources/careers/why/Confidentiality) to review the Confidentiality Statement before advancing to the next slide to complete the module.