



ECU HIPAA Privacy Training

What are the HIPAA Privacy and Security Rules?

- Federal laws that govern the use and disclosure of health information of our patients and research study subjects
- At East Carolina University, these rules apply to (i) any health care provider who submits claims in standardized electronic form for payment; and (ii) any health plan.
 - Also applies to the business associates of these providers and health plans.

What Information is Protected under HIPAA?

- Information that is created or received in the course of providing treatment, obtaining payment for services or performing research; and
- Relates to the (i) past, present or future physical or mental health or condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present, or future payment for the provision of health care to an individual.
 - Includes information in any medium – verbal, written or electronic
- This information is called “protected health information” (PHI) under HIPAA

Notice of Privacy Practices

- In order for ECU providers to be able to use and disclose PHI, each patient must be given the “Notice of Privacy Practices” (NPP) at his or her first visit
- The NPP describes how ECU may use and disclose a patient’s PHI and advises the patient of his/her privacy rights
- NPPs must be posted in all service delivery areas
- ECU must attempt to document the patient’s receipt of the NPP
 - ECU Physicians has an IDX field to populate information indicating whether an NPP has been received by the patient. The cover of the NPP must be sent to Health Information Systems/Services and it is scanned in the medical record.
 - Other providers not operating in IDX should try to document that the patient has received the NPP and it must be filed in the patient’s medical record.

Authorization

- For use and disclosure of PHI that is not for treatment, payment, or health care operations (e.g., quality monitoring, etc.), a written authorization is needed from the patient.
 - Example: Disclosures of PHI to a patient's employer, attorney or for research when the UMCIRB has not provided a waiver of authorization.
- HIPAA privacy rules have very specific requirements on the wording that must be put in the authorization.
 - Please do not try and create your own HIPAA authorization – there is a form available on the ECU HIPAA website at <http://www.ecu.edu/cs-dhs/hipaa/customcf/privacy-forms/authorization%20for%20use%20or%20disclosure.pdf>

Requirement to Disclose Only Minimum Necessary Amounts of PHI

- Except for any use or disclosure of PHI for treatment purposes, HIPAA only allows users to access or disclose the least amount of PHI necessary to perform their duties.
 - Example: If an employer with a valid HIPAA authorization requested a particular lab result of a patient, ECU could not disclose the contents of the entire medical record to the employer.

Patient Rights Under HIPAA

- Patients have the following rights under HIPAA:
 - The right to access and obtain a copy of their PHI
 - The right to request an amendment to their PHI
 - The right to request further restrictions on the use and disclosure of their PHI
 - The right to request alternative forms of communication related to their PHI (for example, the right to request to have PHI mailed to a different address, or the right to request that no messages be left on a particular phone line, etc.)
 - The right to an accounting of the disclosures of their PHI
- If a patient makes any of these types of requests, please have the patient complete the applicable forms that can be found on the ECU HIPAA web page at <http://www.ecu.edu/cs-dhs/hipaa/privacy/forms.cfm>

Filing a HIPAA Privacy Complaint

- HIPAA Privacy complaints may be submitted in any manner (in writing, verbal, e-mail) to the ECU HIPAA Privacy Officer (contact information below).
- Any staff or faculty receiving a privacy complaint from a patient should contact the ECU HIPAA Privacy Officer with the relevant information or immediately complete a Privacy Complaint form located at <http://www.ecu.edu/cs-dhs/hipaa/privacy/forms.cfm>.
- Patients are also permitted to file a HIPAA Privacy complaint directly with the federal government (the Department of Health and Human Services Office of Civil Rights).
- The ECU HIPAA Privacy Officer contact information:
Joan A. Kavuru, J.D., R.N.
2W-31 Brody Medical Sciences Building
600 Moye Boulevard
Greenville, NC 27834
(252) 744-5200
kavuruj@ecu.edu
- There will be no intimidation or retaliatory actions against anyone making a complaint in good faith.

Incidental Uses and Disclosures of PHI

- As a practical matter, there is no way to protect every use and disclosure of PHI
- Any use or disclosure that cannot reasonably be prevented and is limited in nature is not prohibited under HIPAA
 - Example: Discussions during teaching rounds; calling out a patient's name in the waiting room; sign-in sheets in clinics.
 - These are permitted, so long as reasonable safeguards are used to protect PHI.

Employee Access to Protected Health Information

- PHI cannot be accessed by any employee except for the sole purpose of performing employment duties and responsibilities
- You cannot access your family's PHI or your own PHI without completing the proper release/authorization forms at ECU Health Information Systems/Services
- You may access PHI only if you have a legitimate business purpose and need the PHI to do your job (e.g., treatment, payment, or health care operations)
- Review of audit trails is used to monitor compliance of employees' access to PHI.
- Inappropriate access to PHI will result in disciplinary action according to the ECU HIPAA policy on sanctions

Disclosure of PHI to a Patient's Family or Friends

- You may disclose PHI to a patient's family or friends who are present with the patient and involved in the patient's care without obtaining an authorization from the patient.
- Professionals can use their professional judgment on whether or not to disclose PHI to a patient's family or friends if the patient is not present with the family or friend or if the patient is not competent to agree to the disclosure.

Faxing PHI

- Fax PHI only when mail delivery is not fast enough to meet the patient's needs.
- Use a cover page which includes a confidentiality notice.
- If you are unsure of whether the receiving fax machine is in a private location, contact the fax recipient and let them know to wait by the machine until you fax the PHI.
- If you are unsure of the fax number, telephone the fax recipient prior to faxing PHI to confirm the fax number.

New State Laws About Collection, Use, or Disclosure of Social Security Numbers

- Social security numbers (SSNs) are considered PHI under HIPAA – however, the collection, use or disclosure of SSNs is now subject to stricter requirements under state law and University policy <http://www.ecu.edu/cs-itcs/policies/ssnpolicy.cfm> .
- SSNs may only be collected, used, and/or disclosed by ECU and its employees as permitted by law and University policy, and only in furtherance of legitimate University business.
- SSNs are no longer permitted to be mailed (including ECU campus mail).
- Any collection, use or disclosure of SSNs must be approved by the University's Identity Theft Protection Committee (ITPC). Forms and instructions about this approval process are available at <http://www.ecu.edu/cs-itcs/ssnresource/forms.cfm>
- If you have any questions about these new requirements, you may email the ITPC at ITPC@ecu.edu

Proper Disposal of PHI

- Shred or properly dispose of all documents containing PHI that are not part of the official medical record.
 - Do not dispose of PHI into the general trash
 - PHI waiting to be shredded should be placed only in secured bins – do not place in any unsecured trash bin even if the trash bin is not located where it's easily accessible to patients.

System Passwords

- Keep your password confidential – do not share it with anyone
- Physicians – do not share your password for any purpose
- It is important to use strong passwords
- If you must write down your password
 - Store it in a secure location
 - Don't store it near your computer

Use and Disclosure of PHI for Research

- Any human subjects research involving the use or disclosure of PHI must have the appropriate research-related HIPAA forms reviewed and approved by the UMCIRB prior to access of any PHI for research purposes.
- Any investigator wishing to access PHI in preparation for research must comply with the policies for “reviews preparatory to research.”
- Any investigator wishing to access PHI for research on decedents must comply with the policies for “research on decedents.”
- HIPAA research policies, procedures and forms are available at <http://www.ecu.edu/irb>

Use and Disclosure of PHI for Fundraising Purposes

- May access only demographic information and dates of service for fundraising purposes. Disease, diagnosis or condition may not be used to develop a fundraising mailing list.
- ECU medical records or IDX billing systems may not be accessed to obtain names of patients who have received a particular form of treatment for the purpose of soliciting those patients for fundraising purposes (either directly asking for donations or asking them to participate in a fundraising event, e.g., Walk for the Cure).
- Must obtain a valid HIPAA authorization from the patient to use any other PHI for fundraising.
- All fundraising material must provide the recipient with a way to opt out of receiving any additional fundraising material.

HIPAA Do's and Don'ts

- Treat all PHI as if you were the patient and it was your personal information. Don't be careless with PHI in any form (verbal, paper or electronic).
- E-mailing of PHI is discouraged; e-mail messages can be intercepted by third parties or mistakenly sent to the wrong e-mail address. Appropriate safeguards must be taken to prevent unauthorized access of PHI before sending PHI via e-mail to locations outside of the ECU internal network (including e-mail to Pitt County Memorial Hospital). Contact the ITCS Helpdesk for assistance.
- Do not share passwords for any purpose.
- Discuss PHI in closed environments, or use a low voice so that others cannot overhear the discussion.
- Do not access any PHI unless you need it to perform your job.

Workstation Security Practices

- You must protect your workstation and the electronic PHI (EPHI) for which you have access from unauthorized access. *Workstations* are defined as desktop computers, laptops, personal digital assistants (PDA), and other electronic devices that you may use to access EPHI. At a minimum:
 - Do not download or install any software not required for your official job duties
 - Do not open email attachments without verifying the sender
 - Ensure that your monitor or display screen containing any EPHI is positioned to prevent viewing by unauthorized individuals.

Workstation Security Practices-Continued

- Log off from your workstation when your shift is complete.
- Ensure that your workstation is locked when unattended.
- Store all media (e.g., diskettes, zip disks, and flash drives) that contain EPHI in a secure location.
- When disposing of media with EPHI, the data must be removed with data sanitizing software or the media must be physically destroyed. Questions concerning the destruction of EPHI should be directed to the University Privacy Officer.
- Visit <http://www.ecu.edu/cs-itcs/itsecurity/safe-computing.cfm>

Wireless Networking and Purchase of Software

- **Wireless Networking and EPHI:** Do not access EPHI over a wireless network, unless the data is encrypted prior to transmission. Two possible encryption alternatives include the University's Citrix system and the University's Virtual Private Network (VPN). Data sent over a wireless network can be captured by unauthorized persons in nearby buildings, parking lots, and streets.
- *Contact ITCS Security Department* prior to purchasing any computing system that will store or transmit EPHI in order to ensure that the system has appropriate security measures in place.

Storing EPHI on Workstations

- Do not store EPHI on your workstation. An alternative is storing the EPHI on a secure server or a secure network storage device such as Piratedrive.
- If your job requires you to store EPHI on your workstation or departmental server, you are required to contact ITCS to receive further instructions related to such storage.

EPHI and Portable Device Security

- Devices must have a “power on password.”
- Label device with contact information.
- Devices storing, accessing or transmitting EPHI must use AES standard encryption for all data that is stored on the device.
- EPHI shall remain on the device only as long as necessary.
- Bluetooth Infrared shall be disabled while connected; network connection must be achieved via ECU’s Network.
- Device must be powered to log-off or power down after 15 minutes of inactivity.

EPHI and Portable Device Security- Continued

- Devices must be capable of using antivirus; must have an antivirus installed and updated to most recent definitions.
- The device must not be shared among others.
- Before transfer of ownership, the device must be securely wiped of all EPHI.
- The device must implement a device reset with data erasure after 5 consecutive failed login attempts.
- Portable devices must be physically secured; user must take steps to prevent the loss or theft of the device.
- Any loss, theft, or suspected unauthorized use of the device must be reported to the ECU Police immediately.

Reporting of Losses or Misuses of PHI

- You must immediately report all losses or misuses of PHI to the ECU HIPAA Privacy Officer or ECU Security Officer
 - Joan A. Kavuru, J.D., R.N., ECU HIPAA Privacy Officer, 744-5200 or kavuruj@ecu.edu
 - Margaret Streeter, ECU HIPAA Security Officer, 328-9000 or streeterm@ecu.edu

Disciplinary Actions

- Employees and students who violate the HIPAA privacy or security policies are subject to disciplinary action up to and including termination.
- Per ECU policy, the type of disciplinary action is based on the level of the HIPAA privacy or security violation.

ECU HIPAA Privacy Violation Levels & Sanctions

■ Violation Level 1

- Failure to demonstrate appropriate care of PHI
- Examples:
 - Failing to log off a computer
 - Leaving PHI in a non-secure location
 - Inappropriate hallway conversation

ECU HIPAA Privacy Violation Levels & Sanctions (Continued)

■ Violation Level 2

- Improper exposure of PHI within the covered entity resulting in no further improper disclosure of PHI.
- Examples:
 - Repeated Level 1 violations
 - Sharing of password with someone who otherwise has a business purpose to view the PHI accessed with your password

ECU HIPAA Privacy Violation Levels & Sanctions (Continued)

■ Violation Level 3

- Improper disclosure of PHI within the covered entity or outside of covered entity
- Repeated Level 2 violations
- Examples:
 - Failing to perform necessary actions to prevent disclosure of PHI

ECU HIPAA Privacy Violation Levels & Sanctions (Continued)

- Violation Level 4
 - Intentional abuse of PHI
 - Examples:
 - Large scale disclosure
 - Use for personal gain



Federal Penalties under HIPAA

■ Civil Penalties

- \$100 per violation up to an annual limit of \$25,000 per individual

• Criminal Penalties

- \$50,000 to \$250,000 monetary penalties
- Prison time – 1 to 10 years, depending on situation

HIPAA Privacy Quiz

Dr. Smith and a nurse were discussing a patient in an elevator filled with people. In the conversation, the patient's last name, diagnosis and prognosis were mentioned. Which is correct?

1. The patient's privacy was protected since no PHI was disclosed.
2. The patient's case should have been discussed in another room, away from other patients, or at least in low voices that could not be overheard.
3. No patients or families should be allowed to use staff elevators to avoid these situations.

Answer is 2: This information is considered PHI. You should take appropriate safeguards not to disclose a patient's PHI in areas where others can potentially overhear your conversation (e.g., elevators, restaurants, the cafeteria, etc.).

HIPAA Privacy Quiz

Your neighbor's mother has been seen at ECU Physicians for a chronic condition. Your neighbor is confused about the recent treatment ordered for her mother. She asks you (because you work at ECU Physicians) to review the medical record to determine whether this new treatment is correct. The neighbor's mother telephones you and states that she doesn't mind if you look in her record. You are not involved in the patient care team. What should you do?

1. Agree to review the record because you personally spoke to the mother and she said it was okay.
2. Ask the nurse supervisor in the clinic to review the record and let you know what's going on with the mother's treatment.
3. Advise the mother to complete a HIPAA authorization and return it to ECU Health Information Systems/Services so you can review the medical record.

Answer is 3: If you are not a part of the patient care team or otherwise need the PHI to perform your job, you cannot access the PHI without a valid HIPAA authorization. The mother's verbal approval is not sufficient to allow disclosure under the HIPAA privacy rules. Also, you should not ask others to disclose PHI to you if you would not be permitted to access such PHI on your own.

HIPAA Privacy Quiz

You are performing research at ECU and are storing PHI from research subjects on a flash drive (external storage device). The flash drive gets stolen and was not password protected. What should you do?

1. Immediately begin to call the study subjects and make them aware that their PHI is now in an unknown location.
2. Do nothing – nobody will be able to understand the information contained on the flash drive and you don't want to get in trouble because you knew the device should have been password protected.
3. Immediately notify the ECU HIPAA Privacy Officer or ECU HIPAA Security Officer and ECU Police.

Answer is 3: You should not begin notifying study subjects yourself nor should you do nothing. Instead, you need to immediately notify the ECU HIPAA Privacy Officer or ECU HIPAA Security Officer and the ECU Police so appropriate actions can be taken. Always password protect any portable electronic devices that contain PHI.

HIPAA Privacy Quiz

You are a teaching physician at ECU. You have been on call for the past 24 hours and are exhausted. Instead of having to document the past history and physical of a patient in the electronic medical record, you decide to allow the medical student to use your password to document for you. Which is correct?

1. This practice is fine because you are telling the medical student word-for-word what to document so you are confident there will be no mistakes.
2. This practice is fine because you are exhausted and you are afraid you will make mistakes in the chart if you document yourself.
3. This practice is not acceptable because it is never permissible to share your password for the electronic medical record for any purpose.

Answer is 3: Regardless of the circumstances, it is never permissible to share your password.

HIPAA Privacy Quiz

You are a nurse in a busy outpatient clinic. You know that any documents containing PHI must be shredded. You and your staff place documents with PHI waiting to be shredded in an open, unsecured bin on the floor in the clinic. Which is correct?

1. This practice is fine because those documents containing PHI are not being placed in the general trash.
2. This practice is not acceptable because the bin is not secured and anyone could access those documents until they are shredded.
3. This practice is fine because you think that no patients go into the area where the open bin is located.

Answer is 2: Even though you think only employees may access the area where the unsecured bin is located, other staff such as housekeeping, maintenance, or outside vendors may have access to the area and thus the bin should be secured.

HIPAA Privacy Quiz

This year your co-worker got you a great gift for your birthday. You want to make sure you remember your co-worker's birthday this year and you are too embarrassed to ask her yourself. Instead, you go into her electronic medical record to find out her date of birth. Which is correct?

1. This practice is fine because you would look silly asking your co-worker her date of birth.
2. This practice is fine because you are only looking at her date of birth and not any medical information.
3. This practice is not allowed under any circumstance because you do not need this information to perform your job.

The answer is 3: The date of birth is considered PHI even if you do not access any other medical information. Do not access anyone's medical record unless you need information within that medical record to perform your job. Remember, you would probably not want your co-workers looking in your medical record for any reason if they were not involved in your care.

HIPAA Privacy Quiz

A patient has been referred to ECU Physicians for specialty care. ECU Physicians requests the patient's records from the patient's primary care physician. True or False: The patient's records can be disclosed to us without a HIPAA authorization.

The answer is true. Since the records are being disclosed for treatment purposes, no HIPAA authorization is required. Furthermore, the minimum necessary rule does not apply since this disclosure is for treatment purposes (and therefore the entire medical record could be released – not just the parts necessary for the patient's specialty care).

HIPAA Privacy Quiz

Following a visit at ECU Physicians, a patient voices a privacy complaint to the front desk person at the clinic. What should the ECU employee do?

1. Complete a Privacy Complaint Form and forward it to the Privacy Officer or telephone the Privacy Officer about the complaint.
2. Do nothing and hope the patient will forget about his complaint.
3. Instruct the patient to wait until he comes in for his next appointment to make the complaint.
4. Attempt to resolve the complaint on your own.

The answer is 1: All privacy complaints should be forwarded onto the ECU HIPAA Privacy Officer, Joan Kavuru, who can be reached at 744-5200 or kavuruj@ecu.edu. Do not attempt to resolve the complaint on your own.

HIPAA Privacy Quiz

Your mother is a patient at ECU Physicians. She asks you to go into her medical record and print out her lab results and you agree to do it. What is the correct choice below?

1. This practice is acceptable because your mother gave you verbal permission to access her medical record.
2. You are an employee and thus do not have to go through the same procedures as patients do to obtain copies of medical records.
3. You should tell your mother that you cannot access her record until she completes a Release of Information form and submits that form to ECU Health Information Systems/Services (HIS/S). HIS/S will then provide her with the necessary information.

The answer is 3: Employees need to follow the same rules and procedures for access to family medical records just like any other patient – even if there is verbal permission from the family member.

HIPAA Privacy Quiz

Mrs. Jones is a member of your church and is being seen at ECU Physicians for a chronic condition. You are a part of Mrs. Jones' patient care team. You regularly see Mrs. Jones at the clinic and have in-depth knowledge about her condition. Someone at your church knows you work for ECU Physicians and asks you about Mrs. Jones' health condition because Mrs. Jones hasn't been at church in awhile. How should you respond?

1. Tell the individual the latest update on Mrs. Jones' condition because you just saw her in the clinic that previous week.
2. Tell the individual how Mrs. Jones is doing because you know Mrs. Jones would not mind if the church members knew of the recent changes in her condition.
3. Explain to the individual that you cannot comment on Mrs. Jones' health condition and that the individual should ask Mrs. Jones herself about her health condition.

The answer is 3: Because this disclosure is not for the purpose of treatment, payment, or health care operations, Mrs. Jones would need to complete a HIPAA authorization before you could disclose information about her health condition to outside individuals not involved in her care.

HIPAA Privacy Quiz

True or False: At ECU Physicians, a patient's billing record is considered PHI.

The answer is true. Any information related to a patient's care or condition, including payment information, is considered PHI.

HIPAA Privacy Quiz

A co-worker has been admitted to Pitt County Memorial Hospital. You are very concerned about his condition. You decide to check his medical record to make sure he is okay and to find out what room he is located in so you can visit.

True or False: Access to the medical record in this case is a HIPAA privacy violation since you have no authorization from the co-worker for you to access the record and you have no valid business purpose to access the record.

Answer: True. You are never permitted to access anyone's medical record unless it is required for your job or you have an authorization from the patient.

East Carolina University 2008 HIPAA Privacy Training

Quiz Certification

Print Name:

Signature:

Date:

Academic Dept/Program:

To print this acknowledgement
of training go to:

File-Print-Current Slide-OK