



EAST TENNESSEE STATE
UNIVERSITY

HIPAA Compliance



EAST TENNESSEE STATE
UNIVERSITY

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that sets national standards for the protection of sensitive information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened by the Health Information Technology for Economic and Clinical Health Act (HITECH).

In January of 2013, the Department of Health and Human Services issued the “Final Rule” implementing HITECH’s statutory amendments to HIPAA.

This training module focuses on the primary requirements of the HIPAA Rules as amended by the HITECH Act and ETSU/MEAC policies adopted in accordance therewith.

Section 1: The HIPAA Privacy Rule

Section 2: The HIPAA Security Rule



HIPAA Basics

The standards and requirements set forth in the HIPAA Rules apply to the following “covered entities”:

1. A health plan.
2. A healthcare clearinghouse.
3. A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

The HIPAA rules also apply to “business associates” of covered entities.

4. A business associate is a person or entity who performs certain services on behalf of a covered entity that requires them to access, create, receive, maintain or transmit individually identifiable health information.



HIPAA Privacy Rule Highlights



Protecting the Privacy of PHI

ETSU Departments and ETSU/MEAC Clinics that are subject to HIPAA have a duty to protect our patients' health information in all forms. Improper use or disclosure of protected health information can result in harm to our patients and embarrassment to the University.

Breaches of information privacy and security can result in criminal and civil penalties for both the University and the offending employee. Employees will also be subject to disciplinary action by the University/MEAC up to and including termination, as well as liability under Tennessee state law.



What is protected?

Protected Health Information: The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether printed, spoken, or electronic.

The Privacy Rule calls this information "protected health information (PHI)."

- PHI includes individually identifiable health information including demographic data, that relates to:
 - the individual's past, present or future physical or mental health or condition;
 - the provision of healthcare to the individual; or
 - the past, present, or future payment for the provision of healthcare to the individual.

Common examples of PHI: name, address, date of birth, social security number, diagnosis, prognosis, medical record number, payment information, insurance ID number, identities of a patient's relative, photographs, patient's email address, etc.



We must protect PHI in all forms

Printed



- Daily Schedule
- Check-in Forms
- Paper Charts or Rxs
- Patient Billing Statements
- Paper Fax Documents
- Insurance EOB's
- Reports
- Patient Clinical Summary
- List of Patient Names and Addresses

Spoken



- Telephone Conversations with a Patient
- Conversations Between Providers re: a Patient
- In-person Conversations with a Patient
- Calling the Patient's Name in the Lobby

Electronic



- Electronic Medical Records
- Email
- Text Message
- Files Stored in Electronic Form on a flash drive, CD, DVD
- Recordings

Who can access PHI?

A workforce member of an ETSU Department or ETSU/MEAC Clinic must only access a patient's protected health information when doing so is necessary to perform their job duties.

A member of our workforce that accesses a patient's protected health information without a job-related reason for doing so violates the HIPAA rules and will be subject to sanctions.

Case example: A court ordered Walgreens to pay \$1.44 million to a customer whose PHI was **inappropriately accessed** and disclosed by a pharmacy employee. An employee suspected her husband had contracted an STD from his mistress. The Walgreens employee accessed the mistress' medical records to confirm her suspicion, and then shared the mistress' diagnosis with her husband.

Even though the pharmacy employee was authorized to access the pharmacy EMR, she had **no job-related justification for accessing** the mistress' medical records. Additionally, the disclosure of the mistress' PHI to the employee's husband was not authorized by the patient or otherwise required by law.



Access to PHI

If you are a workforce member of an ETSU Department or ETSU/MEAC Clinic and you are also a patient of an ETSU/MEAC Clinic you must follow proper protocol in order to obtain your own medical record!

Remember, just because you have the ability to access a record does not mean you are authorized under the law to do so. **You are only authorized to access protected health information when necessary to perform your job!**

Inappropriately accessing protected health information is a HIPAA violation.



Access to PHI

Accessing PHI without a job related reason for doing so is a HIPAA Violation!



- You are **prohibited** from accessing your own medical record within the EMR. You must follow the proper protocol to receive a copy of your medical record or access the same in your patient portal.
- You are **prohibited** from accessing the medical record of your family members (e.g., spouse, dependents) within the EMR. You must follow proper protocol to obtain a copy of a patient's medical record.



Inappropriate Access

Community Hospital of San Bernardino

- Hospital employee accessed e-PHI of 204 patients “without a clinical need for information”

\$250,000 fine

Over \$1,000 per patient medical record the employee accessed inappropriately



HIPAA and Research Data

The HIPAA Rules regulate how protected health information may be obtained and used for research purposes. This is true whether the PHI is completely identifiable or partially de-identified in a limited data set.

In order to use PHI for research purposes appropriate HIPAA documentation must be obtained, including either:

1. Individual patient authorization; or
2. Approved waiver of authorization from the IRB

HIPAA requirements for accessing and using PHI for research can be found on the University's IRB website:

<http://www.etsu.edu/irb/policies/procedures.php>



Uses and Disclosures of PHI

The HIPAA rules address various conditions under which a patient's PHI is to be used or disclosed.

- Permitted Use/Disclosure
- Required Use/Disclosure
- Patient Authorized Use/Disclosure



Permitted Uses and Disclosures of PHI

A covered entity is permitted to use or disclose protected health information for the following purposes:

- For Treatment
- For Payment
- For healthcare Operations

Disclosures for “TPO” purposes do not require a provider to obtain authorization from the patient.



Required Uses and Disclosures of PHI

A covered entity is required to disclose protected health information:

- To the patient when requested
 - State Law requires a healthcare provider to provide a patient a copy of the patient's medical records within ten (10) business days of receipt of such a request in writing. It does not matter if the patient has an outstanding account balance.
- To the Secretary of the Department of Health and Human Services in relation to an investigation

Disclosures **required** by law do not require a provider to obtain authorization from the patient.



Other Permitted/Required Uses or Disclosures of PHI

- **In response to a subpoena:** The law is very specific when it comes to what PHI can be disclosed in response to a subpoena.**If reasonable under the circumstances, it is best to call the HIPAA Office prior to disclosing PHI pursuant to a subpoena.
- **To a public health authority:** Certain medical information must be reported by law to public health authorities even if the patient doesn't want the information reported e.g. reportable communicable diseases.
- **To police:** Certain wounds or injuries must be reported to police e.g. gun shot wounds.
- **To a state agency:** When a physician or other provider suspects child or elder abuse they must report it to state agencies.

When using or disclosing PHI under any circumstances always do so in compliance with the Minimum Necessary Standard.



Authorized Uses and Disclosures of PHI

Except as otherwise permitted or required by the HIPAA Rules, a covered entity must not use or disclose protected health information absent a **valid authorization** obtained from the patient.

ETSU approved forms can be acquired from the HIPAA Compliance Officer or found on our website.

ETSU HIPAA Compliance Officer:

Lindsay A. Daniel 423.439.8528

MEAC HIPAA Compliance Officer:

Beth Ann Henley 423.433.6050



-
- Treatment
 - Payment
 - Healthcare Operations

Permitted
Use/Disclosure

- To the patient
- To the Secretary of HHS
- To public health agencies and law enforcement

Required
Use/Disclosure

- For most any other purpose not listed above

Requires a
Valid
Authorization



When in doubt...

Call the HIPAA Compliance Office!

Never release patient health information if you are unsure if the HIPAA requirements are satisfied!



We are here to help!



EAST TENNESSEE STATE
UNIVERSITY

HIPAA Security Rule Highlights



What is Protected?

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, PHI. **The HIPAA Security Rule protects a subset of PHI that a covered entity creates, receives, maintains or transmits in electronic form.** The Security Rule calls this information “electronic protected health information” (e-PHI).

The Security Rule does not apply to PHI transmitted orally or in writing.

Common examples of e-PHI: emails that contain PHI, files saved on your computer/laptop/tablet that contain PHI, files saved on shared network drives that contain PHI, electronic medical records, digital photographs of patients, files on flash drives/DVDs/CDs that contain PHI, electronic schedules or calendars that contain PHI, text messages, etc.



What does the law require?

HIPAA requires us to **safeguard the confidentiality, integrity and availability of e-PHI.**

1. Confidentiality: e-PHI is not available or disclosed to unauthorized persons
2. Integrity: e-PHI is not altered or destroyed in an unauthorized manner
3. Availability: e-PHI is accessible and usable on demand by an authorized person

We are required to identify and protect against reasonably anticipated threats to our e-PHI!



THREAT: MALWARE

Viruses, worms, spyware, and spam are examples of malicious software known as “malware.” Malware is any program or file that is designed to infiltrate and damage computers without the user’s consent. Malware can alter or delete e-PHI and precautions must be taken to reduce the risk of malware infection.

THREAT: PHISHING EMAILS

Phishing email scams are fraudulent emails that appear to come from a legitimate source such as your bank, ETSU ITS, the government, etc. These messages generally direct you to a fake website or otherwise attempt to get you to divulge private information such as your user names and passwords, bank account information, social security numbers etc. **ETSU/MEAC Personnel should be suspicious of all unexpected e-mails, even e-mails which don't appear to be selling anything.**

If you have any reason to believe your computer has been compromised, you should immediately contact the HIPAA Compliance Office and ETSU ITS! You should also immediately log off and disconnect your device from the network.



How to Identify Phishing Emails

- The email requests private information
 - ETSU ITS will never ask for your password via email
 - Our EMR vendors will never ask for your username or password via email
- The email indicates you have won the lottery or a free vacation
 - If it sounds too good to be true it probably is!
- The email is from a person or company that you never provided your email address to
- The email contains a hyperlink with a web address that is different than the company's established website
- The email contains grammatical errors or misspellings

If you receive a suspicious email and you are unsure of its legitimacy, you can should contact the ITS helpdesk at itshelp@etsu.edu

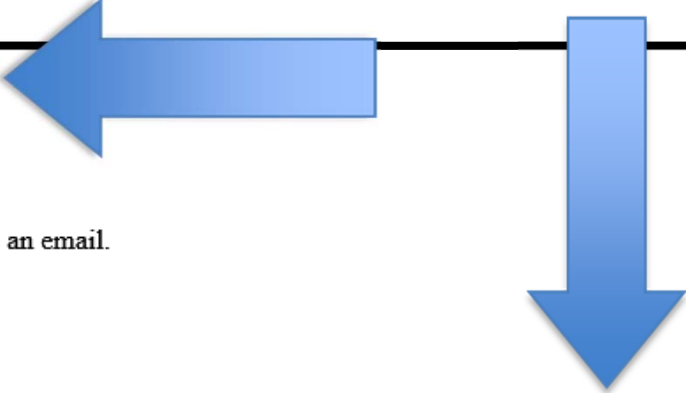


How to Identify Phishing Emails Cont.

- The email indicates you have to take an urgent action in order to get your tax information or in order for you to get paid by ETSU
- The email indicates you have to take an urgent action in order to keep your email mailbox
- The email is from the Dean or your supervisor but not from their ETSU email account
 - May ask for something
 - May be very vague (e.g. Available?)
 - May be marked as urgent



How to Identify Phishing Emails Cont.



From: William Block <gbadebot001@gmail.com>
Sent: Tuesday, February 25, 2020 2:50 PM
To: Guitreau, Shannon <GUITREAU@mail.etsu.edu>
Subject: [EXTERNAL] Request

When you get a minute, could you please drop me an email.

Best Regards
William A. Block
Vice President for Clinical Affairs and Dean

The [EXTERNAL] tag in the subject line identifies emails that do NOT originate from an ETSU person or service. Please exercise caution when handling emails from external sources. Any email that is unsolicited and requires you to take immediate action, appears to be forged or is PHISHING for information can be verified by emailing the ITS Help Desk.



How to Identify Phishing Emails Cont.

From: IT <IT@mail.etsu.edu>
Sent: Monday, May 11, 2020 10:24:11 AM
To: Gage, Donna D. <FORRESTD@mail.etsu.edu>
Subject: [EXTERNAL] Password Check Required Immediately

To All Employees,

As part of ongoing efforts to maintain regulatory compliance we have updated our password policy and we need everyone to check their password immediately.

Please click here to do that:

[Check Password](#)

Please do this right away.

Thanks!



The [EXTERNAL] tag in the subject line identifies emails that do NOT originate from an ETSU person or service. Please exercise caution when handling emails from external sources. Any email that is unsolicited and requires you to take immediate action, appears to be forged or is PHISHING for information can be verified by emailing the ITS Help Desk.



Malware Infection

University of Washington Medicine

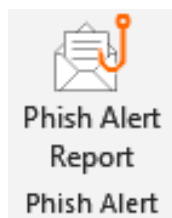
- 1 physician's computer
- Clicked on a link in an email and downloaded malware to his computer
- Malware compromised unknown number of patients' data

\$750,000 dollar settlement with OCR



Reporting Phishing Emails

- When in doubt – report the phish!
 - Do not click on links or open attachments
 - Do not reply to the email
 - Notify ITS by emailing the HelpDesk or simply click the Phish Alert Button on the questionable email



SAFEGUARD: ANTIVIRUS SOFTWARE

ETSU-owned computers are furnished with antivirus software. Laptop users must periodically login to the ETSU network to ensure software is up-to-date. If you must use a personal device to access our EMR you must provide your own up-to-date anti-virus software.

SAFEGUARD: WEB BROWSING

ETSU/MEAC Personnel must not access the internet except for business related sites necessary to carry out effective patient treatment, education, and management while within the remote desktop session inside the EMR environment.

SAFEGUARD: EMAIL

ETSU/MEAC Personnel must not access email while within the remote desktop session inside the EMR environment. We must be diligent in opening and downloading emails and attachments on all devices that access our EMR and ensure emails are legitimate before opening.



Transmission of e-PHI

When possible, **electronic protected health information should be transmitted within the secure confines of the electronic medical record (EMR)**. Our EMR systems provide secure direct messaging capabilities that should be utilized.

All e-PHI that is not transmitted within the EMR environment must be transmitted securely or not at all!



Internal Email Communications (@etsu.edu to @etsu.edu):

- Simply type the word **encrypt** anywhere in the subject line to encrypt the contents of the message and the message attachments
- Do *not* include protected health information in the subject line as the subject line itself is *not* secure

Encrypted messages sent internally will show up in the ETSU inbox and look completely normal—no actions have to be taken to decrypt/read the message.

When the recipient takes subsequent action with an encrypted email (e.g. replies or forwards it) the subsequent emails will remain encrypted so long as **encrypt**—remains in the subject line.



This does not apply to emails directed to patients—see the full text of the Email with Patients HIPAA Policy on the HIPAA website.



External Email Communications (@etsu.edu to @msha.com, etc.):

- Simply type the word **encrypt** anywhere in the subject line to encrypt the contents of the message and the message attachments
- Do *not* include protected health information in the subject line as the subject line itself is *not* secure

Encrypted messages sent from an etsu.edu address to an external address will show up in the recipient's mailbox and require extra steps—recipient will have to follow instructions to access contents of the encrypted message within a secure portal session.



This does not apply to emails directed to patients—see the full text of the Email with Patients HIPAA Policy on the HIPAA website.



FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Cut Copy Format Painter Clipboard

Arial Narrow 12 A A

B I U ab A

Basic Text

Address Book Names Check Names Attach File

To... Lindsay Daniel

Cc...

Send

Subject Schedule Updates **Encrypt**

Lindsay,

Patient John Smith, DOB 04-11-1992 cancelled his afternoon appointment. I scheduled Patient Andrea Roberts, DOB 01-19-1986 in his place.

This email satisfies the HIPAA email requirements!

- ✓ Trigger word **encrypt** in the Subject Line
- ✓ No PHI in Subject Line

Email with Patients

- Patients have a right to receive communications re: their healthcare via unencrypted email
- ETSU Personnel must advise patients who wish to receive such communications of the risks associated with unencrypted email and have the patient sign the appropriate consent form
 - The HIPAA Compliance Office has created an Email Fact Sheet and Consent Form for you to use
- ETSU Personnel should have patients sign the consent form prior to communicating with the patient via email



Summary of Email Rules

Email with Providers, Staff and members of the healthcare team

- ✓ Trigger word **encrypt** in the subject
- ✓ No PHI in the subject

Email must be encrypted.
Encrypt must remain in the subject line when replying, forwarding, etc.

Email with Patients

- ✓ Risks explained and signed consent obtained

Email with patients is unencrypted. No further action required.



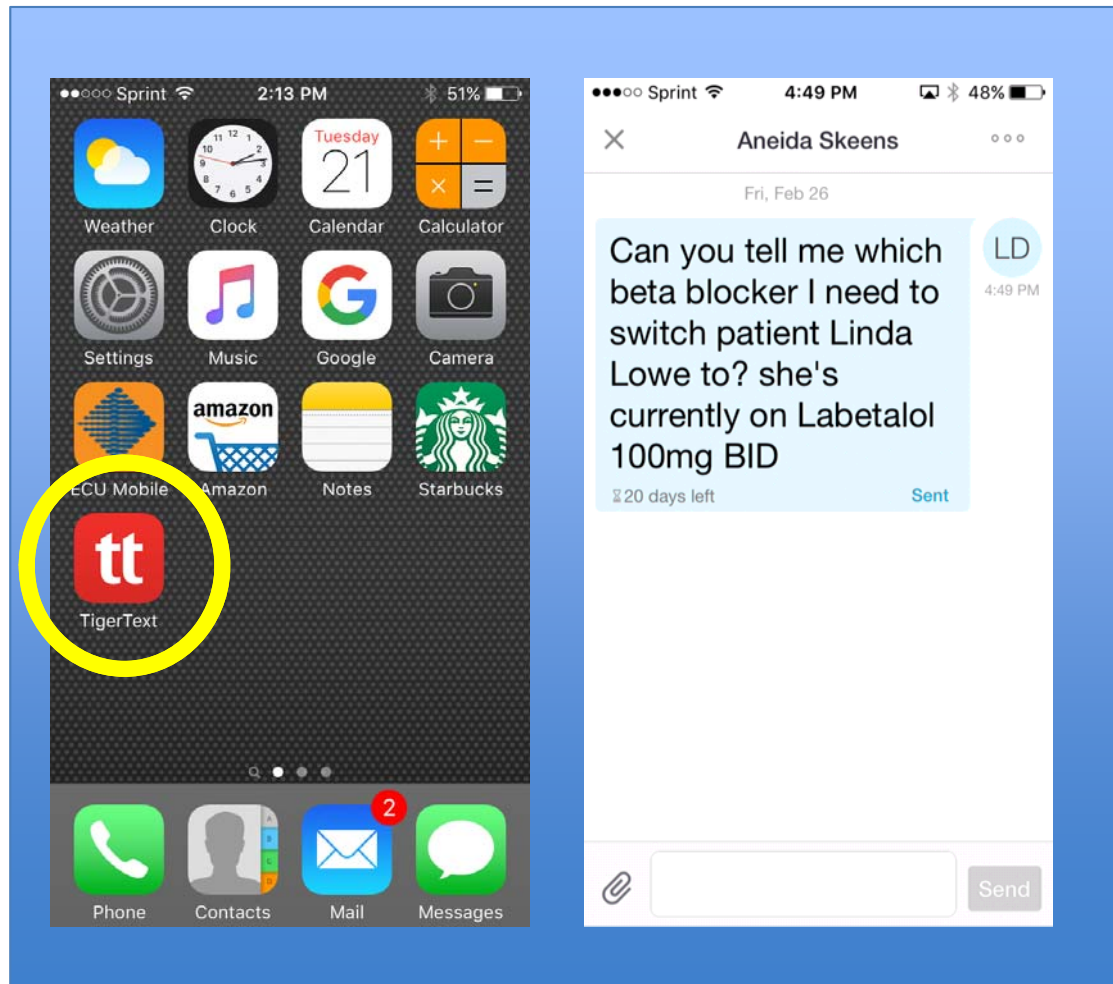
e-PHI **should never be transmitted via SMS text.** Text messages are inherently unsecure.

- We cannot control who views the message
- SMS text messages become part of the sender's and receiver's cell phone records
- SMS text messages can be intercepted in transmission

University assigned TigerConnect accounts enable HIPAA compliant messaging between our providers, staff and administration. To request an account visit the HIPAA Compliance website and fill out the "Account Request Form." **Use of any texting app without approval from the HIPAA Compliance Office is a HIPAA violation.**



TigerConnect



- Used for secure communication of PHI with the healthcare team
- Photos, videos, voice files and other data that contains PHI must be captured and sent within the TigerConnect application
- Full guidelines can be found on the HIPAA website

TigerConnect cannot be used at VA clinical facilities.



Storage of e-PHI

When possible, **electronic protected health information should be stored within the secure confines of the electronic medical record (EMR).** Our EMR systems provide extra layers of security.

All e-PHI that is not stored within the EMR environment must be stored securely! If you have questions about secure storage contact the HIPAA Compliance Office.



e-PHI and Mobile Devices

While convenient, mobile devices are one of the biggest threats to the security of our e-PHI!

In addition to other threats, laptops, tablets and smartphones are uniquely susceptible to loss and theft. The best way to protect our patients' e-PHI and protect ourselves from liability is to:

- ✓ Safeguard all files containing e-PHI outside the EMR environment with password encryption
- ✓ Safeguard all mobile devices by ensuring they are not left unattended

When possible devices should be fully encrypted and remote wiping should be enabled. All devices that access e-PHI must be password protected.



e-PHI and Mobile Devices

Never leave a laptop, iPad or other device such as your smart phone that contains or accesses e-PHI unattended in your bag or vehicle!

When you must transport a device that contains e-PHI it must be done in a secure manner.

When not in use all mobile devices must be securely stored.



Stolen Laptop

Springfield Missouri Physical Therapy Center

- 1 laptop Stolen from a provider's vehicle
- Contained e-PHI of 148 patients

\$1.7 million dollar settlement with OCR



Reporting a Potential or Known Breach

Suspected breaches of privacy or security of protected health information should be **immediately reported** to your supervisor and the HIPAA Compliance Office.

Lindsay A. Daniel

Associate Counsel
ETSU HIPAA Compliance Officer
hipaa@etsu.edu

PHONE:
423.439.8533



EAST TENNESSEE STATE
UNIVERSITY

Lost or Stolen Devices

Immediately report lost or stolen electronic devices e.g. computers, smart phones, flash drives, CDs/DVDs, etc. to the HIPAA Compliance Office and Information Technology Services.



Resources

Department of Health and Human Services:

<https://www.hhs.gov/ocr/privacy/>

HealthIT:

<https://www.healthit.gov/providers-professionals/ehr-privacy-security>

ETSU HIPAA Compliance Office:

<https://www.etsu.edu/universitycounsel/hipaa/>

