TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

HIPAA PRIVACY & SECURITY QUICK TIPS

Why Does Privacy & Security Matter?

Here at Texas Tech University Health Sciences Center we value our patients' rights regarding their privacy and confidentiality.

Ensuring privacy and security of private health information, including electronic medical records (EMR) is a key component to building trust with our TTUHSC patients.

If our patients lack trust in the physical or electronic exchange of their information, it may negatively affect that patient-provider relationship.

What exactly are we protecting?

- Protected Health Information (PHI)
- Both Physical (PHI) and Electronic (e-PHI); and
- Private Information (PI) or Electronic Private Information (e-PI)

Health Insurance Portability and Accountability Act - HIPAA

(http://www.ttuhsc.edu/hsc/op/op52/op5202.pdf)

- HIPAA ensures the protection of a patient's health information and TTUHSC follows this federal law to ensure the privacy and security of this PHI or e-PHI
- PHI is at risk from *YOU* when you access this private information (PI) outside of your job duties, save unsecured/unencrypted PI onto portable devices, do not have updated McAfee Anti-Virus protection on all devices or leave a device *unsecured* in the open, visible to anyone

Information Privacy and Security

There are Information Technology (IT) and Compliance/HIPAA Policies and Procedures that have been implemented based on Federal and State laws and regulations to provide a common framework for adopting and deploying Privacy and Security resources within TTUHSC.

- **Compliance Policies**: http://www.ttuhsc.edu/HSC/OP/op52/
- **IT Security Policies:** http://www.ttuhsc.edu/it/policy/
- **HIPAA Policies**: http://www.ttuhsc.edu/hipaa/policies_procedures.aspx
- **HIPAA Violation Severity Levels and Corresponding Disciplinary Actions:** http://www.ttuhsc.edu/hsc/op/op52/op5214.pdf

Our Patients' Trust Starts With You

ONLY look at, discuss and/or use a patient's PHI/e-PHI if you immediately need it to perform your job duty

- Under HIPAA it is against the law to access PHI or ask someone to access it for you - if you are not authorized or have no business purpose to see PHI to directly perform your job duties
  – *even if you are trying to be helpful!!*

If any other individual outside your department or TTUHSC is requesting PHI, you must first obtain a signed authorization from your patient (ROI) and keep it on file

- Every employee here at TTUHSC ***does not*** automatically have unrestricted access to all PHI across the board. Protect PHI from TTUHSC ***employees who are not authorized*** or do not have any need to see a patient's PHI to perform their job duties

Be discreet in your conversations or when discussing PHI, especially in public areas.

Privacy of PHI

- Don't leave PHI where it is visible or accessible to public or other individuals out in the open
- Use Confidentiality Disclaimer on any fax coversheet
- **PHI/e-PHI is "unsecured" if it is NOT: 1. Encrypted or 2. Destroyed (http://www.ttuhsc.edu/hsc/op/op56/op5604.pdf)**
- Always lock your computer when you walk away from it! No excuses!
  - Ctrl + Alt + Delete, then select "Lock Computer
  - Windows Button + L, and the screen will lock
- Keep offices and workstations secured at all times

Password Security

- *Do NOT ever share your passwords*
  - No one inside or outside our TTUHSC system should ask for it – don't give it out!
  - Do NOT write your passwords down where they can be found!
- Put password protection on all devices and computers that can access PHI
- Make sure all PHI is stored only on Secured Servers
- If your password has been compromised, change it immediately!

HIPAA PRIVACY & SECURITY QUICK TIPS

- If anyone asks for your TTUHSC Unique User ID or password, report it to IT immediately @ ITSolutions@ttuhsc.edu

Anti-Virus Protection

- McAfee is available to all TTUHSC employees for FREE from our IT department
- Must be put onto all devices used from TTUHSC and all devices used to VPN into our network to protect against Viruses and Worms that can compromise our TTUHSC network.

Email Security

- **Phishing** – are emails that falsely claim to be from a legitimate organization with fraudulent intent
    - If you receive a phishing email, do NOT respond and forward the entire email to ITSolutions@ttuhsc.edu
- **Spam** – is unsolicited, unwanted bulk or junk mail
    - To reduce the amount of spam your TTUHSC inbox receives, restrict your use of this email account to business use ONLY
- **Email Encryption** (HSC OP 56.04)
    - When you transmit any PHI or private information (sensitive or confidential) to and/or from a NON-TTUHSC email address, it MUST be manually encrypted
    - Simply place the phrase "[Send Secure]" or "[SS]" into the beginning of the Subject Line

TTUHSC Owned Property and Equipment

Your TTUHSC Computer and/or Laptops and stored electronic data are state owned resources and are NOT for personal use. Using these resources for personal use can put our network at risk. Please don't misuse these resources. Remember you are responsible for violations with your e-Raider ID.

Missing, Lost, or Stolen TTUHSC computing devices must be reported *immediately* to either the Institutional Security Officer (ISO) and/or Institutional Privacy Officer (IPO)

– **AS SOON AS YOU KNOW ITS MISSING!**
(http://www.ttuhsc.edu/hsc/op/op63/op6310.pdf)

It is possible after a violation or breach that the IPO or ISO may restrict all your access to our TTUHSC network to protect our institution.

Financial Penalties for Non-Compliance

- Can you afford the fines ***(up to $1,500,000)*** for a privacy and/or security violation? Fines are the same at Federal and State level. *See below for more details:*

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

How to Report Non-Compliance of HIPAA Privacy & Security Policy and Procedures
(http://www.ttuhsc.edu/hsc/op/op52/op5204.pdf)

- Report to your Direct Supervisor
- TTUS Compliance Hotline
    - 866-294-9352
    - www.ethicspoint.com
  (http://www.ttuhsc.edu/hsc/op/op52/op5203.pdf)
- Contact your Privacy or Security Officers

Institutional Privacy Officer (IPO)	
Sonya Castro-Quirino, AVP Sonya.Castro@ttuhsc.edu	(806) 743-3950
Institutional Security Officer (ISO)	
Andrew Howard Andrew.Howard@ttuhsc.edu	(806) 743-7103
Regional Privacy Officers	
Sherri Johnston - Lubbock Privacy Officer Sherri.Johnston@ttuhsc.edu	(806) 743-4007
VACANT - Amarillo Privacy Officer John.Geist@ttuhsc.edu	(806) 743-9539
VACANT - Permian Basin Privacy Officer John.Geist@ttuhsc.edu	(806) 743-9539