HIPAA Considerations When Working from Home

With a large number of TTUHSC's faculty and staff working from home, the TTUHSC Office of Institutional Compliance would like to remind you of some at-home safeguards when working with Protected Health Information (PHI).

We recommend the following:

- Follow HIPAA Minimum Necessary Standards. When using or disclosing PHI or when requesting PHI, please limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- Only work on PHI in your home. Do not take PHI (including electronic PHI) to a public place, such as a coffee shop or a park.
- Do not store PHI on your local computer/laptop/tablet or USB flash drives at home.
- Encrypt and password-protect all devices that you may use to access PHI. Do not record login information (i.e., username and password) on or near electronic devices.
- Protect inadvertent viewing and sharing of PHI; whether it's through the sharing of a personal computer/device or leaving PHI out in plain view.
- Use caution not to print PHI of any type. If your job requires you to maintain PHI, please use extra caution and shred all copies after use.
- Employees are discouraged to use hard copy (paper) PHI, however employees who have the need to use hard copy (paper) PHI in their home need a lockable desk, lockable file cabinet or safe to store the information. Avoid leaving sensitive documents unattended, especially in high traffic areas. Please shred paper PHI when no longer in use. Use a cross cut shredder to shred documents. Documents should not be thrown into a trash receptacle.
- Protect PHI from family members or friends this includes electronic or paper PHI. Do not discuss PHI with your family members or friends.
- Always lock your computer/devices when you walk away, especially while you are working from home.
- Manually encrypt any PHI or private information (sensitive or confidential) going to a non -TTUHSC email address. Simply place the phrase "[Send

Secure]" or "[SS]" into the beginning of the Subject Line and the email will be encrypted. Don't forget to include the brackets.

- Keep your physical workspace secure; if possible, designate an area in your house as your workspace.
- If you need to discuss PHI or confidential information over the phone ensure you do so in a private area where others cannot overhear you.
- Laptops and flash drives that are not in use should be secured/locked away.
- If a laptop, device, or item that contains PHI is lost or stolen, immediately contact your Supervisor as well as the Privacy/Compliance and Information Security Offices.
- Use of text messaging between mobile devices to discuss any PHI, sensitive or confidential information is not permitted unless through a secure text platform.
- Secure your home wireless network with the following:
    - Change the default administrator password of your wireless router.
    - Set up a strong password for connecting to your wireless network. This password should be different from the administrator password.
    - Allow only people that you trust to connect to your wireless network.
- Make sure each of your computers, mobile devices, programs, and apps are running the latest version of its software.

Please contact Sherri Johnston at 806-743-4007 if you have any HIPAA questions.

April 3, 2020