### https://sagoknowbe4assets.z21.web.core.windows.net/tamus-oit-banner-sm.jpg

### HIPAA Security Tips to Remember

**HIPAA**, or the Health Insurance Portability & Accountability Act (HIPAA) is a civil rights law, which gives patients control over the use and disclosure of their health information. If you work in the healthcare field, you are required to ensure the privacy and security of your patients’ protected health information (PHI).

Communications in your daily work (whether electronic, written, or oral) about your patients can contain sensitive information which is protected by HIPAA. A patient’s protected health information should only be used or released if absolutely necessary for treatment, payment, or healthcare operations, in order to provide adequate care and fulfill your responsibilities as a health care provider.

**Strengthen your HIPAA compliance skills! Follow these tips:**

* Documents containing patient information should be discarded in a shredding container.
* CD-ROMs, USBs and other digital storage should be discarded of carefully – ask your supervisor or manager how you can properly dispose of these.
* If you see any suspicious activity appearing on your computer, report it to your Help Desk or IT team immediately.
* Do not leave messages concerning a patient's health information on answering machines or voicemails.
* Access only electronic information that you "need to know" to perform your job. If you don't need the information for your job responsibilities, do not seek it out.
* Log-off your computer when away from your workstation.
* Lock laptop computers and other mobile devices in a secure location when not in use.
* Store passwords in secured areas only - not accessible by others (no post-its underneath your keyboard or on your computer!)

Employees who do not take care of sensitive information can lead their organizations into fines, increased operating costs, loss of customer confidence, and even more governmental regulation. Do your part to keep sensitive information safe at all times.

The tips included in this message are meant to remind you to keep sensitive information secure. Remember, your organization's privacy, security and compliance policies for handling sensitive information should be followed first and foremost.

**Stop Look Think - before you click.​**