HIPAA FACT SHEET 2023

TMCAH. and all its companies are committed to providing information to help all employees operate and manage our businesses while we maintain regulatory compliance standards regarding all components of protected health information (PHI). A periodic review of Privacy Standards will help us ensure we meet the spirit of the Privacy Practices Intent(s).

**What is HIPAA Compliance?** The Health Insurance and Portability Accountability Act (HIPAA) was passed into law in 2002. The Privacy Rule (The Standards for Privacy of Individually Identifiable Health Information) established a set of national standards for the protection of certain health information. It addresses the use and disclosure of individuals’ health information by healthcare providers or organizations.

HIPAA compliance is a very serious issue and can result in fines of up to **$250,000**. In fact, individual health care workers have been fined from $50,000 to $100,000. Medical providers need trained staff who understand how to properly handle PHI and should set security standards for sensitive data, so everyone understands the fundamentals and what is at risk.

**HIPAA Compliance: Best Practices**

* + Do not share sensitive PHI with others who should not have access, including co-workers, acquaintances, or individual whom the patient has not given access rights to the information. This standard includes digital, emailed, printed, or spoken information.
	+ Avoid accessing a patient’s record unless needed for work. Users will be assigned different levels of security clearance based upon roles and need to know.
	+ Secure all paperwork containing PHI by placing it in a drawer or folder when not in use. Cover charts so patient names are not visible. When faxing, use a cover sheet and confirm with the receiving party that they have received the documents. Never leave records and other PHI unattended.
	+ Close computer programs containing patient information when not in use. Do not leave computer unattended unless the screen is locked.
	+ When emailing PHI encryption must be used. When sending new email from Outlook to a non-Tufts entity use the following steps:
		- from within the email click the File menu,



* + - then choose the Encrypt this Item icon it has a drop down menu, from the drop down menu choose the Encrypt Only option.

 

* + Limit e-mail transmissions of PHI to only those circumstances when the information cannot be sent another way. Encrypt email and only send information via company official equipment. Do not use personal devices to send PHI even encrypted.
	+ Use of unapproved personal devices to access PHI is forbidden by TMCAH.
	+ Text messaging on personal devices can be used only for weather alerts, meeting reminders or similar information but NEVER for patient information.
	+ Never share passwords between staff members. Always use a strong password that is at least eight characters in length, contains at least one capital letter, digit, and special character if the computer program allows.
	+ Properly dispose of information containing PHI by shredding paper files or formatting disk drives. Never store PHI on USB devices.

***References:***

*Department of Health and Human Services HIPAA*. (2015). Retrieved from <http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-> vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf

*Georgetown Law Policy Institute State Law*. (2015). Retrieved from <http://hpi.georgetown.edu/privacy/records.html>

*Health Information Privacy*. (2015). Retrieved from [www.hhs.gov/ocr/privacy/index.html](http://www.hhs.gov/ocr/privacy/index.html)

*HiTech - Public Law*. (2015). Retrieved from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf>