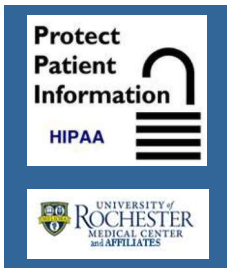
HIPAA HIGHLIGHTS



May 2021

Storing Protected Health Information Electronically

As part of our job responsibilities we are often required to store PHI electronically. Here is a brief view of some of the many ways we do so and how we can make sure the information remains private and secure.

Portable Media

When using portable media such as CDs, DVDs, USB drives, external hard drives or other portable storage, it is essential that the devices and media be encrypted. We have had incidents in the past where PHI was lost as a result of the portable media not being encrypted. Please refer to the URMC and Affiliates HIPAA Security 0SEC06 and 0SEC10 Policies and Procedures for more details on encryption requirements.

Laptops

Similar to portable media, all laptops that may contain PHI are required to be encrypted. As almost all devices used at the Medical Center and Affiliates contain PHI, this is a requirement of all laptops at URMC and Affiliates. Please refer to the 0SEC06 and 0SEC10 Policies and Procedures.

Network Storage

When storing data on the URMC and Affiliates network, it is important to ensure only the right people have access to this data. Please work with your IT Support when setting up network share drives to ensure the access granted is the minimum privilege necessary. Refer to URMC and Affiliates HIPAA Security Policy 0SEC01 for guidance on the requirements for granting access to systems and data.

Cloud Services

Protected Health Information (PHI) is never allowed to be stored in any "cloud" or similar third-party-hosted Internet solution without a proper business associate agreement. Below are a few examples of websites and cloud services where URMC & Affiliates PHI is **NOT APPROVED FOR USE**:

Dropbox	Mozy	FlipDrive
Google Docs	RackSpace	iStorage
Apple iCloud	Evernote	OpenDrive
Files Anywhere	Carbonite	SugarSync
Storegate	FreeDrive	And MANY MORE!
	Pastebin	

URMC and Affiliates has Business Associate Agreements with select cloud services, such as Box.com, Amazon and Microsoft. Only your IT Support can create accounts for you that fall under this agreement. Personal accounts on these platforms are not acceptable for PHI storage. Please contact your IT Support if you need to use this service. Remember, sharing sensitive information outside our organization without proper authorization is a breach.

Please contact the Information Security Office or your IT Support for guidance on which services have been approved for use and how to go about setting up accounts with these companies. Contact your HIPAA Security Official for any questions you might have on the requirements for storing PHI in any form. This is just a basic guide so please do not hesitate to ask any questions.

If you have any questions, please contact your Privacy Officer or HIPAA Security Official or refer to the URMC intranet site at http://sites.mc.rochester.edu/departments/hipaa/.