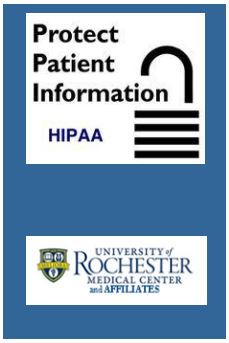
HIPAA HIGHLIGHTS

May 2022



Workforce Member Information Security Responsibilities

The Information Security Office of the University of Rochester has put protections in place to protect URMC and Affiliates from Information Security Incidents. Even with all of these protections in place, attackers adapt new attacks and methods to exploit our resources and data. Our workforce members (YOU!) are our most important line of defense against the threats to our information systems and data. Below are some of your responsibilities as a workforce member.

Reporting of Security Incidents

All workforce members have a responsibility to report any security incident, potential incident, or weakness to their supervisor or directly to the HIPAA Privacy or Security Offices. If you're unsure if something a potential incident, let us know and we can help!

Passwords and Logins

You are responsible for ANY access made with your account. You are responsible for creating a strong password. URMC and Affiliates have requirements that all workforce members must follow:

- **DO NOT SHARE YOUR PASSWORD!**
- Do not write down or store your password (e.g., paper, software file or hand-held device) unless this can be stored securely and the method of storing has been approved by the Information Security Office.
- Change your passwords whenever there is any indication of possible system or password compromise.
- Do not provide your password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks). The Help Desk will not ask for your password!
- Do not use the same password for business and nonbusiness purposes.
- Select strong passwords (see requirements in 0SEC01, Section 01.d)

Presentations

The best way to protect URMC and Affiliates data in presentations is to only include de-identified data when presenting. Workforce members may be required to create presentations that contain sensitive information. It is important to remember that you are required to protect data regardless of where it resides. This includes presentation workstations and the sending of presentations. After presentations are finished, please make sure the data is removed from the presentation workstation.

Encrypting Devices

All URMC and Affiliates workforce members are required to use encryption on all devices storing PHI and other High Risk Data in accordance with federal regulations and UR/URMC & Affiliates Policy. Devices must be encrypted regardless if they are personally owned or provided by URMC and Affiliates. They include, but are not limited to:

- Laptop Computers
- Desktop Computers
- Tablets and Smartphones
- USB Drives (Thumb Drives, USB Keys, Flash Drive, etc.)
- External Hard Drives
- Optical Media (CDs, DVDs, BluRays)

While these are just some of the items, you MUST encrypt all devices and media when the device stores URMC and Affiliates PHI. If you have questions as to whether your device is encrypted, please contact your Help Desk.

Disposal of Assets

All departments and workforce members of URMC and Affiliates are responsible to dispose of anything containing protected health information so that it is rendered unreadable and unrecoverable. Departments and staff are still responsible, and will be held accountable, for custody of sensitive information until the proper disposal handoff occurs.

The best way to dispose of electronic equipment at any URMC and Affiliates location is to contact the University of Rochester IT Equipment Recovery Program. More information is located on their website at https://www.rochester.edu/it/recycle/. **They will come to your location to pick up the equipment!** To schedule a pickup of equipment, complete the form on their website at https://tech.rochester.edu/forms/request-a-pickup/.

As a workforce member of URMC and Affiliates these are just some of the many responsibilities you must be aware of when using computers and technology. For additional information on any HIPAA-related topics, please refer to the URMC intranet site at https://sites.mc.rochester.edu/departments/hipaa/ or contact your Privacy Officer or HIPAA Security Official at http://sites.mc.rochester.edu/departments/hipaa/faqs-resources/hipaa-privacy-officers-and-security-officials/.