HIPAA HIGHLIGHTS

Protect Patient Information HIPAA

UNIVERSITY of ROCHESTER MEDICAL CENTER and AFFILIATES

June 2022

Remote Workers Must Protect PHI

As more workforce members choose to work remotely part-time or full-time, the risks to patient privacy increase. Documents or files containing protected health information (PHI) potentially are exposed to more people in more places. Workforce members have a heightened responsibility to protect patient privacy, in return for the privilege of working remotely.

Follow good privacy and cyber habits when working remotely:

- Keep your physical workspace secure; employ measures to prevent inadvertent viewing and sharing of PHI.
    - Position your computer screen so that other household members can't see PHI that is displayed while you are working.
    - Don't share your passwords with other household members.
    - Stepping away from your work area? Lock your screen using Ctrl Alt Del and select Lock. When you return and sign back in your information is right where you left it!
- 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.
- Use of hard copy (paper) PHI at home is discouraged, however employees who must use hard copy (paper) PHI in their home need a lockable file cabinet or safe to store the information. PHI must be locked or otherwise inaccessible by members of you household when you finish work for the day. If you step away during your work time, don't leave paper PHI in plain view.
- When you are finished working with hard copy PHI, shred it if there is no other need for it. If it must be retained (e.g. for your department) but you no longer need it, onsite storage at URMC and Affiliates is preferred.
- Printing at home is discouraged, but if it has been approved as part of your job function, do not send files containing PHI to a home printer. Use only URMC-managed printers that are configured to print via the secure network.
- Do not forward work e-mails to your personal e-mail. Don't save files or data locally on personal computers (e.g. "Documents" folder) or to unencrypted flash drives. Use shared drives or your H drive; these are secure.
- Protect your laptop and other devices when transporting them. Don't leave them unattended in public places, and hide them from plain view in vehicles (e.g. store in a locked trunk).

Remember that you are responsible for everything that happens in your remote work space, whether it be access by others to paper documents or to electronic files. If your work space is not secure and someone other than you sees or discloses PHI in records you are working on, you have created a potential HIPAA breach that may require notification of affected patients and result in disciplinary action for you, up to and including termination.

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/.