

Reminder: Maintaining HIPAA guidelines crucial for employees working remotely

The Office for Civil Rights, a component of the U.S. Department of State, enforces the Privacy Rule and Security Rule of the Health Insurance Portability and Accountability Act (HIPAA), which merit special consideration for the many WVU Medicine employees who are working from home during the COVID-19 pandemic.

Confidentiality of patient information is of utmost importance and employees are expected to take the necessary steps to protect it at all times.

Any breach of patient confidentiality will result in disciplinary action.

WVU Medicine employees:

- are still responsible to abide by all privacy regulations no matter their work location, onsite or remote
- must adhere to the WVU Medicine Confidentiality and Security Agreement. Refer to WVUHS Policy VIII.221S: Information Access Control and Confidentiality and Security Agreement

Guidelines for remote workforce:

- Ensure your PC and monitor are in a secure, private location in your home away from main living areas and out of the view of family, friends, or others not authorized to see such information
- Participate in conference calls containing PHI in a private location in your home out of hearing range of family, friends, or others not authorized to hear such information
- Practice ‘minimum necessary’ standards at all times
- Do not print Protected Health Information (PHI) from your home
- Computer must be locked anytime an employee steps away, assuring that PHI is not viewable
- Sign off of your PC when workday is complete
- Do not send PHI via email unless it is to a secure email site
- Any PHI in printed format, (notes taken via conference call, etc.) should be protected and disposed of in a secure manner. This can be done by shredding or placing in a secure envelope in a secure location until such time as you can return to work to shred or properly dispose

Refer any specific privacy questions to wvumnopp@wvumedicine.org.