HIPAA AND WORKING REMOTE

Security and Privacy Requirements

- Only authorized remote access users are permitted remote access to any of Tomah Health's computer systems, computer networks, and/or information, and must adhere to all of Tomah Health policies.
- It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect Tomah Health's network when access is no longer needed to perform job responsibilities.
- Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or organizationally sensitive information.
- Remote users must work in a private and physically secure location (i.e. a private room with door and ability to secure/lock door). This location must ensure that others are unable to hear conversations.
- Remote access users must take necessary precautions to secure all Tomah Health's equipment and proprietary information in their possession.

Security and Privacy Requirements

- Virus Protection software and/or malware protection is installed on all Tomah Health's computers and is set to update based on the Organization requirements. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may **not** stop the update process for Virus Protection or Malware Protection on the organization's or the remote user's workstation.
- Copying or photographing of confidential information, including ePHI, to personal media (hard drive, USB, cd, etc.) is strictly prohibited.
- Tomah Health maintains logs of all activities performed by remote access users while connected to Tomah Health's network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 90 days will be disabled.
- Remote access users are automatically disconnected from Tomah Health's network when there is no recognized activity for 35 minutes. Re-authentication is also required every 9.5 hours.
- It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their username or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

Electronic Data Security

- Users may not send any ePHI via e-mail outside of the organization (anything other than @tomahhealth.org email) unless it is encrypted. There are exceptions for the HIM dept. releasing information per HIPAA Privacy Rule. HIM dept. staff are trained on this concept.

Paper Document Security

- Remote users are should not print paper documents that contain PHI.
- Internet of Things (IOT): Voice activated devices (such as Alexa/Echo, etc.) should be disabled when communicating via teleconferencing or when in confidential conversations regarding Tomah Health business.

Enforcement

- Remote access users who violate these requirements are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract.