Privacy Facts #7

Off-Net Clinical Activity Privacy And Security Considerations

OTN sites and health care providers carrying out clinical activities through OTN's "Off-Net" (Non-Virtual Private Network (VPN)) solution have unique privacy challenges. In order to minimize the risk of unintentional and unauthorized disclosure of personal health information, the following best practices should be considered when conducting an off-net event.

How to Prevent this Privacy Breach

- All activity has to be scheduled through OTN. Call 1-866-454-6861.
- Off-Net systems have the ability to host multiple endpoints in the same call. Users must ensure this does not happen when in a conference with OTN as there is risk of dual connection scenario arising:

Patient ↔ Provider ↔ Outside Party

This has a serious potential for a privacy breach as other sites may intentionally or accidentally connect to your event.

It is strongly recommended that Members:

- select “Incoming MCU Calls Off” or “Multipoint Disable” at all times;
- turn off/unplug systems in multi-purpose rooms when they are not in use;
- disable the “enable snapshot” and “remote video streaming” settings. Both features could allow an unauthorized person to monitor a clinical or confidential session by connecting to the endpoint remotely over the network;
- enable the auto-answer “off” or auto-answer point-to-point “no” when systems are being used for clinical or confidential applications in physically secure rooms.

Members are reminded to follow any policies and procedures in place within your facility that:

- ensure the physical security of workstation, and the electronic security of personal health information;
- ensure the collection, use, disclosure, retention and destruction of personal health information is done in accordance with “Personal Health Information Protection Act, 2004” (PHIPA) and any other applicable law;
- ensure compliance with all relevant safety laws, regulations, and codes for technology and technical safety.
- If you suspect a privacy and/or security breach, report the suspected incident to your Chief Privacy Officer or someone acting in that capacity. If working in a Telemedicine environment and a data breach occurs, please contact privacy@otn.ca.

Note: If you are unclear about any of the technical terminology or how to make any of the recommended configurations, please contact OTN’s Service Desk at 1-866-454-6861 for immediate assistance.

References:
End Point Security Guideline; otn.ca/Members/Privacy Toolkit/Resources/Guidelines

Glossary of terms:
VPN (Virtual Private Network) is a computer network that is layered on top of an underlying computer network. The private nature of a VPN means that the data travelling over the VPN is not generally visible to, or is encapsulated from, the underlying network traffic.

MCU (Multipoint Control Unit) The piece of equipment that facilitates the communication of three or more sites in a videoconference