Guideline

Section: Security	**Number:** 21.10.G.v4
Subject: Videoconferencing End-Point Guideline	**Associated Document Form Number:** N/A
Effective Date: Aug, 2007	**Last Reviewed Date:** November, 2018
Last Revised Date: November 2018	**Next Review Date:** November, 2019

PURPOSE

OTN offers videoconferencing services to enable healthcare providers to conduct virtual patient consultations, participate in distance education, and administrative meetings. OTN offers two forms of videoconferencing.

Traditional Organizational videoconferencing securely operates over a combined private and public network by encrypting the videoconferencing system end-points. It can be deployed into traditional room-based studios, work, or home offices and uses wall mounted, portable or desktop systems on their computers. Personal videoconferencing (PCVC) securely operates over the public internet and uses computers and mobile devices with built-in cameras and microphones.

Unintentional disclosure of confidential information, including personal health information (PHI), may occur if one or more telemedicine videoconferencing system end-points is configured or managed in a way that does not make optimal use of privacy and security features and best practices.

Guidelines below offer considerations for Telemedicine Member site organizations and users to review its videoconferencing system end-point security practices with a view to ensure optimal protection of confidential information over the network.

GUIDELINE

While each Member organization and Telemedicine user participating in videoconferencing activities involving the use of PHI must take responsibility for its protection as prescribed by PHIPA, OTN recommends the implementation of safeguards listed below for ensuring complete system privacy and security.

TRADITIONAL ORGANIZATIONAL VIDEOCONFERENCING CONSIDERATIONS:

1. Videoconferencing end-points must have their encryption (e.g. AES) enabled.

   Note: This ensures the secure transmission of the call between system end-points.

2. Videoconferencing end-points should select “Incoming MCU Calls Off” or “Multipoint Disable”

   Note: There are some Member organizations for which disablement of the above option may not be possible. This could occur in events which are not OTN supported. In this case, it is strongly recommended that this feature, along with the “Do Not Disturb” feature, be enabled only during the required period of time and that it be disabled immediately after use. Failure to disable the on-board bridging option may result in refusal of service by OTN (Please refer to the OTN Technical Service Level Agreement).

3. Videoconferencing end-points should disable video snapshot and video streaming.

   Note: Both features could allow an unauthorized person to monitor a clinical or confidential session by connecting to the videoconferencing endpoint remotely over the network.

4. Videoconferencing end-points deployed in multipurpose rooms should be turned off/unplugged when not in use.

   Note: If this option is employed, the organization's Telemedicine Coordinators (TMC) will be advised when upgrades/maintenance are scheduled. They should then ensure that the system is plugged in and turned on at an appointed time to accommodate the scheduled upgrade/maintenance. They will also need to ensure that the unit is plugged in and available for multipoint and point-to-point calls. Please take into consideration that the Global Address Book (GAB) takes some time to load when the unit is turned on.
   If this option is not practical other compensating controls like pointing the camera to a wall, placing a camera lens, and having the microphone muted should be in place.

5. Videoconferencing end-points in physically secure rooms should have auto-answer disabled (i.e. Auto-answer set to "off" or Auto answer point-to-point set to"no").

   Note: If this option is employed, the TMC will need to be in the room to answer all incoming calls. For this reason, implementing this recommendation should be carefully considered.
   If this option is not practical other compensating controls like pointing the Videoconferencing end-point to a wall, placing a camera lens, and having the microphone muted should be in place.

6. If the auto-answer feature is enabled, Videoconferencing end-points should have the microphone muted (i.e. "Auto-answer mic off" or "auto-answer point-to-point mic-off") and the camera pointed to a place where a person will not be in view when a call comes in.

   Note: Implementing this option will ensure that incoming calls will be automatically connected. However, while the incoming caller will not be able to hear the conversation in the room, the incoming caller will be able to see the participants in the room unless the camera is pointed to an empty part of the room or the camera lens is covered to prevent this. It is important to note that if there is a "preset 0" camera setting available, the camera will automatically point itself according to this setting when a call comes in. If this is the case, the setting should point to an empty part of the room.

7. Manually disconnect the videoconferencing end-points from a call if your session ends early.

PERSONAL VIDEOCONFERENCING CONSIDERATIONS:

1. Confidential videoconferencing sessions should be conducted in a private setting, i.e. avoid the use of public spaces or rooms with windows.
2. Monitor the environment when conducting confidential videoconferencing sessions in potentially unsecure locations (e.g. home).
3. Manually disconnect the PCVC session if your call ends early.
4. If you're in a call with multiple users, the "Lock room" feature should be enabled.

RELATED DOCUMENTS

Subject	**Number**
Acceptable Use of Information Assets	21.05.P