Privacy Facts #2

Even When Your Telemedicine System Does Not Appear To Be In Use, You Could Be Connected

Many OTN sites use one room for clinical, educational and administrative events. Even when the videoconferencing system may not appear to be connected, you could be on camera if your system is set to 'auto-answer-on'. This could lead to a privacy breach if you are with a patient and another site inadvertently connects to your system or it could lead to an embarrassing moment if you are on screen without your knowledge.

How to Prevent this Privacy Breach

- Ensure that you have the auto-answer "off" or "auto-answer point-to-point no" enabled.
- When not in use, a videoconference system used for clinical or confidential events located in a multipurpose room should be turned off and/or unplugged.
- Keep the camera pointed to a place in the room where a person will not be in view.
- Snapshot and remote video streaming settings should be left disabled because both features could allow an unauthorized person to monitor a clinical or confidential session.

See the OTN's "Guideline for Physical Privacy of Patients during a Telemedicine Session" and OTN's "Guidelines for End Point Security" for more information.