Team Name: Regional Telehealth Committee	Reference Number: ORG.2010.PL.004
Team Lead: Executive Director - Mid	Program Area: Telehealth
Approved by: Executive Director - Mid	Policy Section: General
Issue Date: February 27, 2015 Review Date: Revision Date: June 11 2018	Subject: Security and Integrity – Telehealth Equipment

POLICY SUBJECT:
Security and Integrity - Telehealth Equipment

PURPOSE:
To ensure the security and integrity of Telehealth equipment.

BOARD POLICY REFERENCE:
Executive Limitation (EL-01) Global Executive Restraint and Risk Management

POLICY:
The security and integrity of Telehealth equipment and devices is maintained by:
  ➢ Controlling inventory, storage and access,
  ➢ Ensuring appropriate use of equipment,
  ➢ Implementing preventative maintenance,
  ➢ Reporting all equipment issues.

PROCEDURE:
Inventory, Storage and Access
  1. An inventory of equipment and devices is maintained by the Site Manager and MBTelehealth.
  2. Equipment is located in areas that:
       ➢ protects them from extreme conditions, including temperature and moisture
       ➢ can be secured when equipment is not in use, or when area is not attended
  3. The Site Manager is responsible to establish local procedures and assigning responsibilities to secure equipment and control storage and access.

4. Telehealth devices that are particularly vulnerable to damage, loss or theft (including handheld cameras, laptops) require additional security measures and are not to be left in areas that are unattended at any time.
5. The Site Manager is responsible to establish local procedures for storing and facilitating controlled access and return processes for these peripheral devices.

Equipment use

➢ Telehealth equipment and devices are used solely for supporting Telehealth activities, including clinical, educational and administrative sessions.
➢ Providers, staff and clients are supported in the use of Telehealth by site staff within assigned roles and responsibility.
➢ Telehealth users that have been trained may participate or facilitate Telehealth sessions independently.
   • Training includes basic technical, documentation, privacy and security requirements.
   • Users are provided reference material to supplement training as well as the MBTelehealth training materials available at http://www.mbtelehealth.ca/trn-training.html.
   • Users are provided ready access to the MBTelehealth Service Desk phone number and information on the process for obtaining technical assistance before, during or after an event.

Preventative Maintenance, Reporting and Responding to equipment Issues
Telehealth Sites

➢ All Telehealth equipment malfunctions will be reported to MBTelehealth. See MBTelehealth Service Desk Process 6.20.10 (June 2013).
➢ Equipment damage, loss, or theft is documented on a Southern Health-Santé Sud Occurrence Report by any staff member identifying same and reported to their immediate supervisor.
➢ The supervisor forwards the occurrence report to the Site Manager.
➢ The Site Manager notifies the MBTelehealth Facilitator – eHealth Solutions of the issue.
➢ The MBTelehealth Facilitator – eHealth Solutions will report to MBTelehealth Manager, Regional Services.
➢ The Site Manager determines next steps in consultation with their own supervisor, MBTelehealth Facilitator – eHealth Solutions and consults the Southern Health-Santé Sud Executive Director – Telehealth as deemed necessary.

MBTelehealth

➢ Supports a regular preventative maintenance program on equipment.
➢ Supports on-call technical support through the MBTelehealth Service Desk reported incidents
➢ Reviews, analyzes and responds to all reported incidents from the site within a Quality Improvement resolution process.