Care. Connected.

Policy and Procedure

Section: Security	**Number:** 21.35.PP.v2
Subject: AES Encryption	**Associated Document Form Number:** N/A
Effective Date: January, 2010	**Last Reviewed Date:** July, 2014
Last Revised Date: July, 2014	**Next Review Date:** July, 2016

PURPOSE

The Ontario Telemedicine Network (OTN) has an obligation to provide administrative, technical and physical safeguards to ensure the confidentiality and security of personal health information. In particular, these safeguards must protect against unauthorized use and disclosure of any information transmitted across OTN's hardware and software infrastructure.

Encryption is one of the main tools used to protect the confidentiality of information sent over computer networks. As part of its efforts to provide a reasonable level of security to its members, OTN mandates the use of encryption on all Videoconferencing Endpoints (Endpoints). OTN's Videoconferencing Endpoints provide support for the Advanced Encryption Standard (AES), a symmetric key algorithm that is an accepted encryption standard in the United States.

POLICY

All OTN Videoconferencing Endpoints must have AES encryption enabled at all times. Members are expected to maintain compliance as per the OTN Technical Service Level Agreement (TSLA). OTN will actively monitor Endpoints to determine whether AES encryption has been enabled, and will work with Members to ensure that their equipment is configured appropriately. Members who are unable to adapt to OTN's AES encryption policy may be switched to a different network solution.

PROCEDURE

1. OTN has described the standard Videoconference Endpoint configuration in its TLSA. This configuration, which is mandatory for all Endpoints, requires that AES encryption be enabled.
2. All new Endpoints going live with OTN must be configured in accordance with the TSLA.
3. OTN will monitor compliance with this policy in an active manner. The following general mechanisms will be used:
   a) Routine Monitoring: OTN will scan active/live equipment on a routine basis in order to determine whether members are in compliance with this policy.
   b) Event Monitoring: Upon the initiation of an event, OTN will attempt to determine whether AES encryption is enabled on the participating endpoints.
   c) Maintenance and Certification: During routine maintenance of equipment, as well as during certification procedures, OTN will check whether the equipment in question meets the standard Videoconference Endpoint configuration settings..
4. If a Member site's equipment is found to be non-compliant through routine monitoring, OTN will:
   a) Notify the Member site that AES encryption is not enabled;
   b) Work with the Member site to restore the standard configuration on the system; and.
   c) Document the occurrence and share that information with both the Member and the OTN Account Manager.

5. If a Member site's equipment is found to be non-compliant through event monitoring OTN will:
   a) Immediately attempt to notify the site that activity is taking place on an Endpoint which does not have encryption enabled;
   b) Subsequently work with the site to either immediately reset the endpoint, or reboot it at an appropriate time;
   c) Formally notify the Member site in writing of the non-compliance incident
   d) Document the occurrence and assign the OTN Account Manager and OTN privacy/security staff to follow up.
6. If a Member site's equipment is found to be non-compliant at a time when the equipment is being certified or maintained, OTN will document the incident and report it as per the associated guidelines.
7. OTN will monitor non-compliance incidents documented at Service Desk and will identify sites that have repeatedly encountered difficulties fulfilling their obligations under the TSLA.
8. OTN will work with each Member to ensure that all Videoconferencing Endpoints are maintained in standard configuration, as defined in the TSLA.
9. Should a Member be unable to maintain their Videoconference Endpoint in standard configuration, OTN will work with the Member to reach an acceptable solution as per the TSLA. The solution may result in the Member's connection being moved to a gateway solution, rather than the standard on-net integrated infrastructure. Should the need arise to move to a gateway solution, OTN and the Member will work together to determine a solution. In this case, OTN will give the Member 60 days notice of the change.

DEFINITIONS

AES encryption - A symmetric, block-cipher algorithm adopted by the United States government's National Institute of Standards and Technology (NIST).

Gateway Connection - An alternative means for Member sites to connect to the OTN's networks. A gateway connection is similar to OTN's VPN-S connection, but for the fact that the Member site must provide a dedicated virtual local area network within its facility. OTN will install a device that will ensure that all outgoing traffic on this network is encrypted.

Technical Service Level Agreement - An agreement that Member sites must accept in order to use OTNs services. The purpose of the TSLA is to provide a clear description of the services that OTN offers members, as well as to clarify the roles and responsibilities of Member sites.

System certification - A technical process in which new/existing Videoconferencing Endpoints are tested to ensure compliance with OTN technical protocols.

RELATED DOCUMENTS

Subject	Number
AES Non-compliance Report (Event Monitoring).	
AES Non-compliance Report (Routine Monitoring)	
AES Non-compliance Report (Certification & Maintenance)	
AES Encryption Guidelines	