External Telehealth Videoconferencing

“Organization”, as referenced below, is defined as the lower mainland collaboration of Health Authority (HA) Telehealth Programs, consisting of the Provincial Health Services Authority (PHSA) and / or Vancouver Coastal Health (VCH) and / or Providence Health Care (PHC), under the direction of the Lower Mainland Collaboration (LMC) Information Management /Information Technology Services (IMITS).

1.0 Policy Background

Access to telehealth-enabled clinical services can improve and equalize access to high-quality health care services across BC. Appropriate use of telehealth technologies is predicted to improve access to healthcare and scarce health professional resources for a wide range of conditions or services such as general consultation, radiology, pathology or rehabilitation. Telehealth is expected to improve patient-centered care by offering services “closer to home”, while enhancing efficiencies in clinical decision making, treatment planning and mentoring. Telehealth can also avert indirect healthcare costs for both patients and health care providers by reducing the burden of travel for care.

An emerging trend in the video conferencing industry is the proliferation of desktop and mobility video solutions. This trend is also a catalyst for increasing demand by providers and patients seeking ubiquitous access to videoconferencing services to improve timeliness and quality of care, as well as remote attendance of educational or administrative meetings. Whether web-based or client-based (video conference software installed on a computer or mobile device) the majority of these solutions leverage the Internet as a network transport.

B.C. Health Authority enterprise telehealth videoconference systems were designed primarily to service patients and providers within the boundaries of the Health Authority secure networks. While the enterprise systems are technically capable of interaction with external 1 video devices (PCs, mobile device and purpose built video units over the Internet), there are a number of institutional limitations within the Health Authorities that hinder adoption and growth. Limitations include lack of provincial guidelines, specifications and policy.

---

1 The Internet or qualified private networks such as Physician Private Network (PPN)
2.0 Policy Purpose

This policy supports the provincial vision for province-wide access to high-quality healthcare services via ubiquitous audio-visual connectivity when and where it’s needed for health care providers, employees and health service recipients.

This External Video Conference (EVC) Policy provides direction for users of the Organization’s telehealth services to connect with others outside the Enterprise Network Gateway (eNG). This policy provides guidance regarding:

- Video conference network access;
- Clinical consultation processes over video conference;
- Requirements for confidentiality, privacy and confidentiality;
- Roles and responsibilities organizational telehealth programs, Health Shared Services BC; Organizational IMIT departments; telehealth users and telehealth service requestors.

3.0 Effective Date

This policy was approved by PHSA and VCH/PHC Policy & Procedure Committees on May 8, 2014.

4.0 Policy Principles

The guiding principles of this policy ensure that the following key aspects of high quality, trusted telehealth service delivery are considered at all decision points.

1. Support and advocate for optimal clinical and administrative processes using the most appropriate telehealth tools and infrastructure;
2. Protect the confidentiality, privacy and security of clinical transactions and personal health information;
3. Improve the timeliness and quality of health care by bringing services to locations outside health authority networks;
4. Provide optimal service quality (visibility, audibility, connectivity)
5. Ensure flexibility to respond to emerging technologies;
6. Leverage standards-based compatibility with enterprise based video conference systems
7. Achieve provincial consensus for policies, standards and guidelines for seamless business interoperability;
8. Adhere to established standards to telehealth solution quality, interoperability and security; and
9. Mitigate unauthorized system access.

Policy Title: External Telehealth Videoconferencing

Control Area/Category: Information Management Information Technology Services
Reference: IMIT 400
Effective as of: May 8, 2014
Approved by: PHSA and VCH/PHC IMITS Planning & Priorities
Review Date: 
Revision no.
5.0 Policy Statement

Scope

5.1 The scope of this policy refers to video conferencing activities between the BC Health Authority (HA) eNG network and sites external to the network. External sites may connect to eNG via the Internet or Trusted Networks.

5.2 The scope of this policy includes both video conference solutions and software applications that interface with the existing Organizational video conference network and endpoints, as well as point-to-point video conferencing and collaboration solutions.

5.3 All clinical video conferencing events included in the scope of this document must link external sites through the Organization’s video conference infrastructure to ensure appropriate quality, security and technical support.

Organizational Video Conference Network Access

5.4 Video conference events must be initiated by Authorized Users within each Organization’s network or by those using an Organization’s issued devices or video conference software. (e.g.: Organization Employees, Contractors etc.)

5.5 Only Authorized Users can dial directly into the Organization’s network. Participants outside of the eNG network without Organization-issued devices or video conference software must be brought into the Organization’s network by a participant within the Organization’s private network. (e.g.: calls to Community Care, Out-of-Province, Consumers or Patients).

5.5.1 For example, for a clinical consultation the Organization-based consulting site will initiate the call to bring an external patient on-board into the Organization’s private network.

5.6 The Organization must have systems and processes in place to approve the creation of remote video conference accounts.

5.7 Point-to-point video conferences should be scheduled in advance using Organizational Telehealth Management Software or other standard processes to prevent room and equipment scheduling conflicts and privacy breaches.

Clinical consultation over external video conferencing

5.8 The consulting clinician is responsible to select the most appropriate Organizationally-approved and supported video conference hardware or solution to meet their clinical requirements. The Organization’s Telehealth Office will provide guidance regarding appropriateness and interoperability of specific technologies to meet specific clinical requirements.
5.9 Patient privacy and confidentiality must be maintained under all circumstances. Clinical users are responsible to apply the same privacy principles to a Telehealth consult as they would to office visits. (see Privacy and Confidentiality and Proactive Disclosure Procedures Policies)

5.10 Consulting clinicians must adhere to Organizational policies and procedures policies and procedures consistent with face-to-face encounters as it relates to clinical documentation, consent, collection disclosure and storing of information in client’s records.

Confidentiality, Privacy and Security

5.11 All Organization-enabled and supported video conferencing events must be transmitted over encrypted devices for secure end-to-end connectivity. See PHSA Video Conference Standards for minimum encryption standards.

5.12 Video conference technologies and software solutions must comply with local Organizational security policies for network connectivity and data storage.

5.13 It is expected that users will comply with provincial legislation, and Organizational policies and guidelines related to confidentiality and privacy. These include:

5.13.1 BC Freedom of Information and Protection of Privacy Act (FOIPPA) for public bodies and the Personal Information Privacy Act (PIPA) for private and not-for-profit sector organizations providing telehealth services in BC.

5.13.2 Organizations must ensure that externally based videoconference users are familiar with and has agreed to abide by that HA’s privacy and security policies and guidelines.

5.13.3 Organizations must ensure that externally-based video conference users are responsible for ensuring that personal computers and other mobile devices with video conference software are encrypted and physical logical and malware protection is enabled including PIN, auto-locking and anti-virus software.

5.14 Personal/portable video conference technology may not be used in public or unsecure environments.

5.15 Personal/portable video conference technology should be used in a manner that provides privacy, such as a room designed to prevent interruptions or to limit hearing of conversations by individuals not involved in the consultation.

5.16 Video conference events will not be recorded locally on computer or mobile devices.
Technical Accountability

5.17 The Organization is responsible to provide support to users working on Organization-issued hardware and software solutions. The Organization is not responsible for personal computer performance or security management.

5.18 The Organization is not responsible to ensure that connecting networks outside eNG have sufficient bandwidth to meet quality and reliability requirements for telehealth videoconferencing.

6.0 Telehealth Roles and Responsibilities

Telehealth is a collaborative activity requiring the contribution of stakeholders in clinical, business and technical roles. Table 1 below provides a general outline of the roles and responsibilities of Telehealth stakeholders for successful project deployment and sustainment.

Table 1: Telehealth Roles and Responsibilities

<table>
<thead>
<tr>
<th>Organization</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Telehealth Program / Telehealth and Video conference Offices</td>
<td>• Client (end user) requirements and options assessment; solution design, development and implementation; vendor engagement (quotes, installation, training); • Telehealth scheduling and bridging; • Training and operational support; • Provision telehealth facility/endpoint guidelines and standards; • Privacy impact assessments; • Technical support for telehealth events; • Communication with Health Shared Services BC(HSSBC)/Organization Information Management Information Technology (IMIT) for provisioning/de-provisioning user accounts for telehealth information systems;</td>
</tr>
<tr>
<td>Health Shared Services BC (HSSBC)</td>
<td>• Identification of standards for healthcare technologies and security; • Acquisition, delivery and support of standardized desktop and mobile technologies (Service Desk); • Provision of standard data network, voice, video, and collaboration technologies; • Granting and managing access to the bridge management system; • Regular auditing of bridge management access logs • Security assessment and management of bridging infrastructure; • Monitoring of backend technologies (data centres, core communications closets, servers and disk storage);</td>
</tr>
<tr>
<td>Or Organizational IMIT Services department not part of HSSBC</td>
<td></td>
</tr>
</tbody>
</table>

Policy Title: External Telehealth Videoconferencing

Control Area/Category: Information Management Information Technology Services

Reference: IMIT 400

Effective as of: May 8, 2014

Approved by: PHSA and VCH/PHC IMITS Planning & Priorities

Page 5
### Organization

<table>
<thead>
<tr>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical support for network and account management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telehealth-enabled clinical service providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identification and compliance with any specific clinical regulatory requirements associated with telehealth-enabled service delivery;</td>
</tr>
<tr>
<td>• Identification and compliance with clinical best practice guidelines (BPGs) specific to the clinical specialty for the delivery of telehealth-enabled care;</td>
</tr>
<tr>
<td>• Confirm that licensure of service provider(s) is appropriate for both the services provided and is the jurisdiction of the provider and patient;</td>
</tr>
<tr>
<td>• Billing/reimbursement for services rendered is conducted in accordance with MSP Payback Schedule, Preamble, Section D.1. Telehealth Services;</td>
</tr>
<tr>
<td>• Comply with local HA policies and guidelines related to confidentiality and protection of privacy; and</td>
</tr>
<tr>
<td>• Compliance with organizational telehealth policies, guidelines and standards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telehealth service requestors</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Request event scheduling with or without bridging services via the Organizational Telehealth Office.</td>
</tr>
<tr>
<td>• Compliance with organizational policies, guidelines and standards</td>
</tr>
</tbody>
</table>

### 7.0 Related Policies

Organization standards and guidelines can be accessed [here](#) at the PHSA POD.

- Information Security Policy
- Access Management Policy
- Network Acceptable Use Policy
- Network Acceptable Use Agreement
- Remote Access Policy
- Mobile Computing & Device Usage

---

**Policy Title:** External Telehealth Videoconferencing  
**Control Area/Category:** Information Management Information Technology Services  
**Reference:** IMIT 400  
**Effective as of:** May 8, 2014  
**Approved by:** PHSA and VCH/PHC IMITS Planning & Priorities
- Mobile Computer & Portable Storage Device Policy
- Privacy and Confidentiality
- Proactive Disclosure Procedures
- Managing Privacy Breaches Guidelines

8.0 External References

- *BC Freedom of Information and Protection of Privacy Act*
- *BC E-Health (Personal Health Information Access and Protection of Privacy) Act*
- *BC Personal Information Protection Act*
- *MSP Payback Schedule, Preamble, Section D.1. Telehealth Services*

---

2 Vancouver Coastal Health and Providence Health Care have separate Privacy and Confidentiality Guidelines and Guidelines for Managing Privacy Breaches

---

*Policy Title: External Telehealth Videoconferencing*

*Control Area/Category:* Information Management Information Technology Services

*Reference:* IMIT 400

*Effective as of:* May 8, 2014

*Approved by:* PHSA and VCH/PHC IMITS Planning & Priorities

*Review Date:*

*Revision no.*
Appendix 1: Use Case Scenarios

The following use cases describe a sample of scenarios where a clinical telehealth consultation may appropriately take place between Organizational and external endpoints.

1. Emergency Department connecting to clinician at home after hours;
2. Authorized clinician connecting from community-based office to outpatient hospital setting;
3. Authorized clinician connecting to patient in their in home;
4. Authorized clinician connecting to First Nations Community;
5. Authorized clinician connecting to homecare nurses;
6. Authorized clinician to connecting to community-based nurse practitioner;
7. Authorized clinician connecting to other Partner Networks such as Ministry of Child and Family Services or Ministry of Justice;
8. Authorized User joining a videoconference educational or administrative session from a remote site
Appendix 2: Terminology and Definitions

The following terms may be used in this policy or related documents:

**Call Types**

- **Point to Point (Direct)** - One video conference endpoint calls another directly; no bridging infrastructure is used to link the sites.
- **Point to Point (Bridged)** - Two endpoints are connected through bridging infrastructure
- **Multi-point (Direct)** - Multiple endpoints are called directly by one host endpoint using multi-point software on that device
- **Multi-point (Bridged)** - Multiple endpoints are connected via a bridge

**End Point Types**

**Organizational Video Conference Infrastructure**
The current provincial video conference infrastructure is comprised of approved, established and recognized (commissioned) facility-based video conferencing devices and enterprise-based video conferencing applications.

Current infrastructure components include:

- Standards based, fixed room-based videoconferencing unit
- Standards based mobile videoconferencing unit (clinical cart)
- Standards based desktop videoconferencing units
- Desktop computer (or laptop) software based video conferencing standard application

**New Video Conference Technology Offerings**
The following video conference enabled solutions are, or may be, piloted for exploratory test or pilot studies. These may be considered for routine deployment and use. Technologies may include:

- Desktop video conferencing software or other collaboration applications with embedded real-time videoconferencing software;
- Hardware with native embedded video conference technologies such as tablets, mobile phone applications, etc.

**Videoconferencing Event Types**
Although this policy has been created to enable clinical telehealth services connecting people within and outside the Organization’s network infrastructure the following video conference event types are included in the definition of Telehealth services and are subject to the implications of this policy.

- **Clinical** (patient to clinician; clinician to clinician(s))
- **Educational** (clinician to clinician; educator to professional or academic learners; etc.)
- **Administrative** (non-clinical meetings such as corporate, finance; HR; interviews; performance reviews; etc.)

**Other Definitions**

- **“Authorized User”** refers means any staff, individual or application who has been authorized to access and use organization information technology. Typically Authorized Users are provided network accounts to enable authentication.
- **“B.C. Health Authorities”** refers to the organizations primarily responsible for health service delivery as described in the BC Ministry Health Service Plan.
- **“Bridge or Bridging Infrastructure”** refers to technology hardware component used to connect multiple video conference endpoints together in one conference. Also known as a multipoint control unit or MCU.
- **“Consulting Clinician”** is the health care provider using telehealth technologies to provide services over distances.
- **“Enterprise Network Gateway”** (eNG) is the digital network that connects the Health Authorities to each other, to the provincial data centre, and to other Trusted Networks such as the Physician’s Private Network (PPN) and the University of British Columbia (UBC) private network.
- **“External Provider”** means a user of a System who is not affiliated with the Organization and whose access to the System is not for the purpose of performing duties on behalf of the Organization.
- **“Electronic Health Record System”** or “EHR System” means an information system containing or providing access to information about the health of an identifiable individual.
- **“E-Health Act”** means the E-Health (Personal Health Information Access and Protection of Privacy) Act as amended from time to time.
- **“IMIT”** or **“IMITS”** means the Organization’s Information Management/Information Technology (Services) department.
- **“Partner Networks”** refer to private digital networks of partner organizations such as Ministry of Child and Family Services or Ministry of Justice.
- **“Patient”** refers to a patient, resident or client requiring telehealth-enabled health services.
- **“Personal Information”** means any recorded information about an identifiable individual (including, but not limited to patients, clients, residents, volunteers, students, staff,
physicians or members of the public), but it does not include business contact information (business contact information is information such as a person’s title, business telephone number, business address, email or facsimile number).

- **“Staff”** means all officers, directors, employees, contractors, physicians, health care professionals, students, volunteers and other service providers engaged by the Organization.
- **“System”** means any of the Organization’s shared electronic information system.
- **“Telehealth”** refers to the use of information and communications technology – such as video conferencing - to deliver health services, education, and information over distance.
- **“Telehealth Community Solutions”** refers to the use any communication (audio, audio/video) and/or information technology to deliver health services and exchange health information to and from the home (or community) when distance separates the participants.
- **“Telehealth Management Software”** refers to the use of organizational software to book telehealth rooms and equipment, thereby preventing unplanned privacy breaches associated with unscheduled connections. *Telehealth Connect* is the provincial telehealth scheduling application licensed to the BC Heath Enterprise (all Health Authorities) and currently in use in PHSA and VCH.
- **“Trusted Networks”** are other trusted private networks authorized to transmit and receive data through the eNG such as the Physician’s Private Network (PPN) and the University of British Columbia (UBC) private network.
External Telehealth Video Conferencing Standard

"Organization", as referenced below, is defined as Health Shared Services BC (HSSBC)

1. Summary
This External Telehealth Video Conferencing Standard describes technology HSSBC technical standards required for clinical telehealth service activity connecting locations within and outside the Health Authority (HA) Networks

2. Standards
This External Telehealth Video Conferencing Standard supports Vancouver Coastal, Provincial Health Services Authority, and Providence Health Care (VPP) External Telehealth Video Conferencing Policy and VPP External Telehealth Video Conferencing User Guidelines.

2.1. Incoming connections are only accepted by a VCS Expressway under the following circumstances:
   2.1.1. The incoming call originated from a trusted connection in an approved trusted network (e.g.: UBC’s MEDIT/MPAACT; Physician Private Network).
   2.1.2. The incoming call originated from an approved or authenticated source using a provisioned device or video conference software.
   2.1.3. The incoming call is directed to a specific endpoint validated to an exceptions list that will receive unrestricted calls (e.g.: by st. executive request). HSSBC will work with HA’s to determine the appropriate VCS Expressway configuration for the exceptions list.

2.2. Technical Specification Standards for acceptable video conferencing technologies:
   2.2.1. Interoperability Standard: H.323 or SIP Video Conference Compliance
   2.2.2. Encryption Standard: Minimum AES 128 (or appropriate higher level encryption standards as they evolve)
   2.2.3. Transmission Standard: Recommended minimum speed of 512 kb/sec; 30 frames per second.

2.3. Computer/ Mobile Device Technical Specification Requirements:
   2.3.1. Computer/ Mobile Device Technical Specifications are dictated by the video/ collaboration software
   2.3.2. Pretest is required ensure a newly installed video conferencing unit’s capacity to connect and transmit sufficient quality signals for clinical or non-clinical videoconferencing.
2.4. Computer/ Mobile Device Technical Support:
   2.4.1. The local HA service desk will support to users working on Health Authority issued hardware and software solutions. The local HA service desk is not responsible for personal computer security or performance.
   2.4.2. The Health Authority cannot ensure the quality or reliability of video conferencing applications resident on personal computers, or carried on networks outside the Health Authority firewall.
   2.4.3. Users external to the Health Authority Network are responsible to ensure that sufficient bandwidth is available for quality audio and visual signals.

3. Where to Apply This Standard
This standard applies to clinical and non-clinical telehealth service activity connecting locations within and outside the BC Health Authority (HA) Networks.

4. Metrics and Enforcement
HSSBC Unified Communications and the VCC Telehealth teams will enforce this standard through the implementation of new video conferencing solutions adhering to these standard and related policies and user guidelines.

All new implementations must adhere to the standard and current instances will be grandfathered in, where feasible.

5. Exceptions
Exceptions are permitted only in extraordinary circumstances for approved business or clinical purposes. Exceptions can only be approved with the agreement of the HSSBC Provincial Manager Unified Communications and VPP Director, Telehealth.

6. Related Policies
For further related information please refer to the following Lower Mainland IMITS Policies and Standards
   - External Telehealth Video Conferencing Policy
   - External Telehealth Video Conferencing User Guidelines
   - Information Security Policy
   - Network Acceptable Use Policy
   - Remote Access Policy
   - Mobile Computer & Portable Storage Device Policy
   - Access Management Policy
7. Release History and Approvals

Include who must approve changes to the standard and the mechanism for approval, and the roles of those with final approval.

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date of Change</th>
<th>Author</th>
<th>Approvers</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 8, 2013</td>
<td>N. Gabor</td>
<td></td>
<td>Content (reviewed by TAG) placed into standard format.</td>
</tr>
</tbody>
</table>