Australian Government

Department of Health and Ageing

Guidance on Security, Privacy and Technical Specifications for Clinicians

Draft for Consultation

31 August 2011

Disclaimer

The Department of Health and Ageing (DoHA) makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. DoHA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

This document is maintained in electronic form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is draft for consultation, and as such will be subject to change based on feedback provided.

Guidance on Security, Privacy and Technical Specifications for Clinicians

Introduction

This guidance material has been developed through the National Health Chief Information Officer Forum (NHCIOF) Telehealth Cross Jurisdictional Telehealth Reference Group. It has been developed to provide guidance and information relating to security and privacy, interoperability and technical requirements is provided to assist healthcare providers in choosing telehealth (video conference) equipment.

This draft is provided for information, consultation and feedback.

Groups of healthcare providers that are considering participating in telehealth activities may wish to consider opportunities for negotiating bulk purchasing of equipment and some form of aggregated support arrangement (regionally or locally negotiated contracts with suppliers for service establishment and for ongoing technical support). This is highly recommended, and we suggest you contact your State Health's Telehealth department for suitable suppliers and/or advise.

This information has been taken from work commissioned by the various state and territory health departments to provide advice on security, privacy, interoperability and technical requirements for telehealth services.

Videoconferencing Protocol Standards

When choosing your Videoconferencing equipment, whether it be hardware or software based, please ensure that the following specifications and standards are considered. The equipment or software should comply with these standards as a minimum:

- **H.323 Videoconferencing and/or**
- **SIP Videoconferencing**

The following (technical) protocols are used by this equipment to provide interoperability between videoconferencing devices.
H.225 – Call Signalling, Registration, Admission and Status (RAS)
H.245 – Control Signalling
RTP/RTCP – Transmission of audio and video traffic
H.460 – Firewall traversal.
H.239 – dual stream video conferencing capability**Video Codecs**
H.261, H.263, H.263+, H.263 Interlaced, and H.264

Audio Codecs
G.711, G.722, G.722.1, G.728, G.729 including Annex A and B, G.723.1, G.722.1 (Annex C), AAC-LD, and AAC-LC

Encryption

- Advanced Encryption Standard (AES)
- Secure Real-Time Transport Protocol (SRTP) for SIP encryption

If you are uncertain as to whether the equipment meets these standards please speak with your equipment provider.

Other principles

- All equipment should be able to operate according to the agreed standards-based (as listed above), or if proprietary, provide a mechanism to allow audio and video sessions between the proprietary and standards-compliant endpoints;
- To promote interoperability, where standards-based products are proposed, features that are provided by proprietary or pre-standard extensions should be avoided
- Manufacturers should demonstrate interoperability using the stated minimum subset in a heterogeneous environment.

Videoconferencing Equipment Standard Options

For diagnostic or complex clinical management (diagnostic quality VC)

Hardware based videoconferencing solutions are best designed for this outcome.

Many alternative solutions exist and the following technical standards below can be referred to in comparing and selecting alternatives;

- Minimum call speed/bandwidth 384k
- Horizontal resolution: 460 lines (PAL)
- Focus: autofocus
- Optical zoom ratio: minimum 10x
- Standards-based far-end control of pan/tilt/zoom
- For video consultations, to avoid poor performance, round-trip latency must be lower than 300ms. This is dependent on your internet connection and you should consider the upload and download speeds – seek a symmetrical connection which means ADSL 2 or cable
- For video consultations, to avoid poor performance, packet loss should be less than 0.1%
- For clinical consultations, to avoid poor intelligibility, audio should be encoded at a minimum of 16kbit/s

For non-diagnostic and non-complex clinical management (general quality VC)

Hardware based videoconferencing solutions are best designed for this outcome; however software solutions also exist at a lower price point which will also achieve suitable results.
There are a range of alternative solutions and the following technical standards can be referred to in selecting alternatives;

- Minimum call speed/bandwidth 256k
- Minimum resolution: Video Graphics Array (VGA) (640x480)
- Frame rate: 30 frames per second (FPS) (at VGA resolution)

For both diagnostic quality and non-diagnostic (general quality VC)

Please refer to the diagnostic quality list above.

What Not to Buy or assume is appropriate

There are a few software based video conferencing solutions technologies available over the internet, these are generally consumer based technologies and provide functionality which is feature rich, but generally non standards based and of low audio and video quality. This means they are unlikely to be able to connect to a videoconference with someone using a different videoconference solution. Many of these technologies are built around collaboration such as sharing desktops and provide videoconferencing as a secondary function. These are not recommended for providing "Telehealth" video consultations or clinical diagnostics. The other issue frequently experienced with this type of videoconference solution is that there is limited technical and other support – you will need to be able to set up and manage this software yourself as well as identify how to connect to those specialists and others you wish to videoconference with.

When selecting a suitable product please ensure that the above technical standards/protocols are supported and adhered to by the vendor/manufacturer.

Important Principles to Follow

- Higher quality Internet connections provide better videoconferencing quality. Ideally seek a symmetrical connection (where upload and download speeds are the same). This would require as a minimum ADSL2 or equivalent in Cable Internet. Dial-up or ADSL is generally not sufficient.
- Wireless 3G can be a solution but wireless connectivity is variable and can be subject to dropouts and contention. Use only as a last resort alternative solution. Usually 3G cannot sustain 384k videoconference call speeds and as a result may not be suitable for clinical determination.
- High definition videoconferencing requires at least 1.5meg connection – if this is not available or too expensive standard definition is more than suitable for clinical diagnosis.
- Any systems must be "easy to use". Selection of technologies without appropriate training or support from a vendor/manufacturer will be disappointing.
- Factor in hardware/software support for the videoconferencing equipment as part of the initial purchase. Most vendors' couple the software updates to the hardware warranty. In most cases software support is important to maintain standards based capability with new systems. Also consider if the unit fails and is not supported by warranty could you afford to purchase a new unit and get it installed and working in a short timeframe, or wait for a repair to occur. Most warranties include an advance replacement service so you can get a new unit whilst waiting for a repair to occur.
- Consider if the vendor you are purchasing the equipment from can provide remote helpdesk support for general usability issues and or technical support and troubleshooting remotely. There is no point having a solution which you cannot get assistance in connecting to another system over the phone when you need something to be happening at short notice. Generally if you can't get support in 30 seconds – 1minute of making a call you're likely to abandon the session and technology.

- Consider selecting a vendor experienced in videoconferencing and one who can assist with configuration of DMZ and NAT routing for your business internet connection to ensure your VC unit can both connect to other systems, and that other systems can then connect to your unit. Configured incorrectly you may only be able to make calls, not receive them. Often Internet service providers may be able to assist with this setup for an additional fee.
- The vendor should supply training as part of the purchase.
- Individual State Telehealth departments should provide a test facility for prospective vendors and clinicians to test their systems.

Security and privacy

When conducting a Telehealth consultation, as in a physical face to face consultation, there will be a requirement to ensure the consultation is secure and private. To ensure public trust in a teleconsultation, privacy protection and security mechanisms must be integral to any implementation. The following guidelines need to be considered which conducting these consultations:

Policies and procures:

- Telehealth services should be compliant with all relevant state and federal laws.
- Telehealth service providers should periodically review and update their
    - privacy policies;
    - privacy notices; and
    - practices and procedures for managing information, including data security measures

to ensure that they adequately address the management of information gathered during telehealth consultations.

Data Security

Through out a telehealth consultation data will no doubt be transmitted. It is important to ensure that unique identification, authorisation and message security to provide the safest and optimally secure method of exchanging healthcare information. These technologies, known collectively as secure messaging, ensure that the health information exchanged by healthcare providers is protected against malicious interference.

The National eHealth Transition Authority (NEHTA) is currently working with the medical software industry to develop specifications and standards for secure messaging for healthcare providers. This work is associated with the Australian government's Practice Incentives Program.

Health messaging software systems need to conform to NEHTA's technical specifications for secure messaging. Compliance requirements apply to suppliers of health messaging products and services. NEHTA has published a list of eligible suppliers that meet the compliance requirements.

A copy of the secure messaging fact sheet can be found at:

http://nehta.gov.au/component/docman/doc_download/1031-secure-messaging-fact-sheet

Video Conference Security

- The technology standards listed in this document should be configured to require "encryption" of the video traffic as mandatory.
- Hardware based videoconferencing units must support International Telecommunications Union (ITU) H.235 standard allowing encrypted communication between end points in both point-to-point and multi-point videoconferencing sessions.
- Any software based Video Conferencing applications Policy guidelines for the retention and storage of any telehealth recorded consultations could be developed to assist those telehealth service providers which are not subject to specific legislative requirements for the retention and maintenance of health records. Recorded telehealth consultations are subject to the data storage rules applying to all health information.

Other Factors which will impact on the quality of the telehealth consultation:

Items of interest to ensure good VC experience (video and voice) would be:

- Consider the appropriate camera location in room, on desktop etc – background and distance from patient/clinician
- Acoustics, loudness/volume, earphones or speakers, privacy issues
- Documented patient consent
- Need adequate lighting for the room, wall colour, adequate window covers, brightness,
- Simple setup of VC – auto answer on or off ,
- Consider Camera on/off rules – cover camera, mute microphone, etc

Glossary:

interoperability	
proprietary	
ADSL 2	
cable	
Secure Multipart Internet Mail Extensions (S/MIME) Version 3.0	
International Telecommunications Union (ITU) H.235	

Disclaimer

The decision to use, or not to use, telehealth together with the choice of particular hardware or software methods for consultation should rest with the clinician. In making their choices, clinicians should consider any legal (privacy and security), safety and clinical effectiveness implications.