eHealth Ontario
EMR Connectivity Guidelines
Version 1.3 Revised March 3, 2010

Introduction

Ontario's new eHealth strategy includes the use of commercially-available high-speed Internet to meet Electronic Medical Record (EMR) and eHealth connectivity needs for Physician offices. The eHealth Ontario EMR Connectivity Guidelines are intended to ensure physicians have the information they need to make informed decisions about connectivity.

The guidelines, along with the connectivity requirements of both the physician practice and the EMR vendor, will define the minimum connectivity requirements that the practice must consider as part of the selection process.

Many practices already have Internet connectivity in their offices. These guidelines should be used to confirm whether the existing connectivity configuration is adequate for EMR and eHealth activity, or whether changes are required.

Funding

A 3-year subsidy for Internet connectivity is now included for physicians participating in the Physician eHealth EMR Adoption Program.

Physicians selecting an Application Service Provider (ASP) EMR solution will receive additional funding to help cover the cost of a second, redundant Internet connection to address business continuity needs.

Revisions

The connectivity guidelines are also intended to help ensure physicians' EMR systems are able to integrate with provincial eHealth services planned for release over the coming years. The connectivity guidelines may be updated as new requirements and eHealth services are announced. Please refer to the OntarioMD web site regularly to ensure you have the latest version of the guidelines.

Additional Information

The OntarioMD Transition Support Program can provide additional guidance regarding EMR and connectivity requirements for the specific practice implementation. Contact information and program details are available at http://www.ontariomd.com.

Requirement	Description	Practice Checklist
Connection Speed (Bandwidth & Capacity)	Bandwidth requirements will vary significantly based on the size of the practice (e.g. number of EMR users) and the other office connectivity usage requirements. At a minimum, a practice is required to use a Business Grade Broadband Internet connection with the ability to assign static IP addresses. EMR system vendors will specify minimum bandwidth requirements for the specific solution being proposed. The practice's local IT support resource(s) and the EMR vendor must work together to ensure that the practice's total expected Internet usage is considered when calculating bandwidth requirements. The practice should carefully consider connectivity costs as part of their overall EMR planning to ensure that a cost-effective EMR and connectivity option is implemented.	☐ Determine, with EMR vendor, the total required bandwidth ☐ Confirm availability of a suitable Internet connection that meets the connectivity guidelines and practice bandwidth requirements ☐ Perform a cost analysis to ensure that a cost-effective EMR solution and Internet connectivity option are selected
Business Continuity	Practices that select Application Service Provider (ASP) EMR solutions will rely heavily on their Internet connection for day-to-day practice operations. These practices must arrange for a second Internet connection to ensure business continuity in the event of an outage. The second connection would be used in the event that their primary connectivity is temporarily unavailable. Ideally, a second connection should be from a different provider to reduce the likelihood that a specific provider problem may disable both connections. Practices have the option of using both connections simultaneously, or having a primary and secondary	☐ Ensure all Internet/network devices are properly connected to a UPS ☐ For ASP/Hosted solutions, ensure a suitable business continuity solution is in place ☐ Ensure the business continuity solution is tested regularly

	connection, only one of which is used at a given time. Either connection should be available instantly should the other fail, and the practice should arrange to be notified in this situation. Additional network hardware and services will be required to integrate two Internet connections within the practice. Practices that are using a local EMR solution are only required to have a single Internet connection, but may opt for a second connection if business needs so dictate. All Internet connectivity devices, and at least one computer, should be connected to an Uninterruptable Power Supply (UPS) device to ensure ongoing connectivity during a power outage. The UPS should sustain sufficient ongoing connectivity to support the practice's business continuity needs (e.g. powering computers, printers, network devices)	
Acceptable Use	The practice should develop and communicate an Acceptable Use policy governing their practices' use of the Internet. In general practices should limit their use of the Internet to essential business applications for which the risks are understood and acceptable. Physician practices should be familiar with their EMR and/or connectivity vendors' (particularly ASP vendors) Acceptable Use guidelines.	☐ Ensure Acceptable Use Policies exist and are communicated within the practice
Security & Privacy	Physicians are responsible for selecting, implementing and ensuring the effectiveness of safeguards to protect against security threats and inappropriate use. These safeguards are needed to prevent security breaches that may impact: • patient privacy • confidentiality, integrity or availability of practice information and patient records • appropriate and efficient delivery of care by the practice • privacy or security of the broader community, where an attack flows through the practice's Internet connection. The Personal Health Information Protection Act	☐ Ensure hardware and software firewalls are installed, configured and maintained by a knowledgeable person ☐ Ensure Antivirus software is installed and updated on an ongoing basis

	(PHIPA) specifically requires that Personal Health Information (PHI) be protected by technical, procedural and administrative safeguards. Technical safeguards are necessary, but not sufficient. Internet connectivity will always involve security risks. Connection to the Internet increases exposure to malicious software (e.g. viruses, spyware) and numerous other security threats. Practices should limit their use of the Internet to essential business applications for which the risks are understood and acceptable. Practices must ensure that a network security firewall device is installed. Antivirus software and bi-directional software firewalls should be installed on all practice computers. All operating system and application software should be kept up to date by installing vendor updates, service packs, security patches, and new Antivirus signature files. These updates can often be automated. Firewalls should be configured to block all Internet traffic – inbound and outbound – except for traffic that is specifically required to meet business needs. Wherever possible, firewalls should allow connections only from/to specified IP addresses using secure protocols. Inbound connections should only be allowed if there is confidence that safeguards, such as restriction to specific, trusted IP addresses or address ranges, are adequate. Firewall alerts should be sent to a person with the knowledge and responsibility to correct problems and manage incidents. EMR applications should protect the data stream between the client and host using cryptographic controls. A practice can also engage a qualified security consultant / advisor to help ensure that all their security considerations are met.	☐ Ensure computer operating systems and applications are updated with service packs, security patches, etc. ongoing ☐ Ensure the EMR solution protects the data stream between the client and host using strong encryption ☐ Understand and confirm compliance with PHIPA
Secure Remote Access	Practices that use their Internet connectivity to allow staff or business applications to connect to the practice or EMR from remote locations may need additional software, hardware or services from their	☐ If Remote Access is required, ensure that a secure Remote Access

	connectivity vendor, EMR vendor or other supplier. The practice should be familiar with the security requirements associated with remote access to the EMR. For example: • A static IP address from the connectivity vendor • Strong authentication – for example: one-time passwords, security tokens, or cryptographic secrets • Firewall changes to permit access to the practice from the Internet using a secure communications protocol: IPSEC, SSL, or SSH	solution is implemented
Help Desk / Support	Practices should ensure that telephone-based support for connectivity is available during the operating hours of the practice. If staff rely on this connectivity for after hours access then support during these time windows should be considered as well. Practices should also evaluate the response time the connectivity vendor commits to for service issues/outages. Generally, a 24 hour window to resolve issues/outages is the minimum requirement. The connectivity provider should clearly explain what elements of connectivity are included within their support agreement. For example, most connectivity vendors will not provide support for local (in-office) network issues without additional arrangements. By default, most connectivity vendors will be responsible for the wires entering the practice and any network device (e.g. cable or DSL modem) the vendor has supplied, but no more. Ensure the delineation of responsibility is well-understood and that the practice has appropriate IT support in place.	☐ Confirm hours of support ☐ Confirm response time for outages ☐ Confirm scope of connectivity provider and EMR vendor support responsibilities ☐ Confirm support resources assigned to address all practice IT support requirements, including all connectivity considerations

Glossary

Antivirus Software	A software application used to prevent, detect and remove malicious software (such as viruses, worms and spyware) from computers.
ASP EMR	An Electronic Medical Record system that is installed in a remote location (typically eHealth Ontario) and that requires users to access practice/patient information through external network connectivity.
Bandwidth	The maximum data transmission rate supported by a particular Internet connection, usually expressed as bits (or megabits) per second. Download speed (receiving data) and upload speed (sending data) are often different.
Business-grade Internet Connection	A class of service available from Internet connectivity providers that is targeted at businesses, as opposed to consumers. Typically includes improved performance guarantees and/or support services.
Configuration 2 – Hub and Spoke	An EMR configuration where the EMR server is hosted at a physician's office and other group sites access the server securely through external connectivity.
Hardware Firewall	A physical appliance that blocks unauthorized access to the local network from the Internet, while permitting authorized uses.
Local EMR	An Electronic Medical Record system that is installed locally within a physician office and does not require external network connectivity to access practice/patient information.
Local IT Support Resource	A person employed or engaged by the practice to provide assistance with information technology systems, software and devices within the practice. This may include setting up computers and network/Internet services and troubleshooting related problems.
Personal Health Information Protection Act (PHIPA)	The Personal Health Information Protection Act sets out rules for the collection, use and disclosure of personal health information. The full document is available online at the ServiceOntario e-Laws site at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm For a guide to the Act provided by the Information and Privacy Commissioner (IPC) of Ontario please access the IPC site at http://www.ipc.on.ca/images/Resources/hguide-e.pdf

Static IP Address	All devices connected to the Internet have an IP address. IP addresses allow information to be sent to the correct end-point on the Internet. A static IP address is a permanent address provided by an Internet Service Provider. Static IP addresses are manually assigned by the end user to a firewall, router, computer or other connected device. (This contrasts with a dynamic IP address, which is a temporary address assigned automatically when a device connects to the Internet.) A static IP address can facilitate trusted communication between two known end-points on the Internet and provide advantages in setting up applications such as email, web services and remote access.
Software Firewall	A software application, installed on a personal computer, which blocks unauthorized network/Internet connectivity, while permitting authorized uses. A "bi-directional" software firewall controls both inbound and outbound requests to/from a personal computer.
UPS	Uninterruptible Power Supply – a battery backup system that supplies power, for a limited period of time, to office devices (such as computers or network devices) in the event of a power failure.

Appendix A – Additional Technical Information

This appendix provides technical information, recommendations and requirements for the following:

- ISP network circuit type/sizing,
- firewall hardware specifications/ features,
- remote access considerations,

as well as related information regarding
- LAN configuration, and
- local site/facility readiness.

The intended audience for this appendix is a technical IT resource, including local integrators, EMR vendor staff and technology-savvy physicians or their staff.

***** Please Note: It is very important that the physician practice work closely with their EMR vendor to determine EMR bandwidth requirements as well as to identify any additional bandwidth requirements for other applications. Failure to do so can result in impaired application performance of both the EMR application and other applications using the ISP connection.**

Category		Requirements/ Considerations	Additional Rationale	Recommen-dation
ISP Network Circuit & Sizing	Config 1: Local EMR server; serving one site only	Bandwidth/circuit usage calculations should include: ▪ Criticality, frequency and number of users accessing applications over network ▪ Network performance attributes of applications being accessed over the Internet ▪ Remote access usage of EMR application	Practices must ensure that all EMR access methods, including remote access, are considered when confirming required upload and download requirements.	Required

Category		Requirements/ Considerations	Additional Rationale	Recommen-dation
		▪ Network performance attributes of EMR application (Performance information should be available from the vendor)		
	Config 2: Locally hosted EMR server with sites accessing the EMR via external connectivity	Bandwidth/circuit usage calculations for hub sites should include: ▪ Criticality, frequency and number of users accessing EMR and other hub-site-hosted applications over the network ▪ Network performance attributes of EMR application being accessed over the Internet from Spoke sites or remote locations	Upload speed is a significant consideration for the hub site network connection. Considerations for network sizing should include bandwidth upload and download speeds. The EMR Vendor should be asked for network latency requirements to be met by connectivity providers. For a hub site a symmetrical connection like DS1 is strongly recommended to meet both the upload and download demands.	Required
	ASP EMR Config: EMR server is hosted at the eHealth Ontario Data Centre	Consideration should be given to the number of concurrent users accessing the EMR over the Internet from a given site. EMR Application Service Providers to provide specific circuit and bandwidth recommendations for the proposed EMR solution.	Considering the practice usage requirements along with the EMR recommendations will ensure a suitable size circuit is identified. ASP configurations require a second circuit for business continuity. This can be configured in a load-balanced active / active configuration or as a failover.	Required
	IP addressing	At least one static IP address.	A static IP address should be applied to the site's firewall Internet port.	Strongly recommended
Firewall		A hardware-based Firewall appliance must be installed between the Internet provider modem and site	This will reduce risk at the site from inbound internet attacks. Additional Firewall details are provided in this	Required

Category		Requirements/ Considerations	Additional Rationale	Recommen-dation
		LAN equipment.	section.	
	Hardware Specification	Firewall should provide minimum three Ethernet ports.	Minimum one WAN 10/100/1000 Mb Ethernet port, one DMZ port or port that can be used as a DMZ port for connecting external facing server(s), and minimum one LAN port.	Required
	Firewall Feature set	Native VPN capability	For remote access as well as site- to-site connectivity.	Required
	Firewall Feature set	Stateful Inspection Firewall	Allows dynamic packet inspection beyond the header.	Required
	Firewall Feature set	Firewall should protect against a broad range of threats.	These Firewall features include protection against DDos attacks, IP spoofing, synfloods, malformed packets, etc.	Required
	Firewall Feature set	Support of dyndns,org and similar name querie	This feature is important if the ISP network circuit in place can not provide a static IP	Required (if static IP addressing not available)
	Firewall Feature set	Supports Syslog and/or SNMP	Configuration that allows forwarding and storage of logs to a separate server. This will allow historical analysis and auditing	Strongly recommended
	Firewall Feature set	For larger LAN environments the Firewall should support Port-based and Tag-based VLAN, NAT and VIP	These features should be used in larger LAN environments to logically divide the LAN in segments as well as provide access to hosted applications	Strongly Recommended
	Firewall Feature set	Firewall should support secondary/backup ISP.	For business continuity purposes, the firewall should have more than one WAN port and be able to load balance disparate connectivity providers. (ie: Cable and DSL)	Recommended
	Firewall Feature set	Firewall should have Network Monitoring tools built in	This tool should include features like VPN Tunnel Monitor, Connection Monitor, Network Activity Monitor, Local Logs, Traffic	Recommended

Category		Requirements/ Considerations	Additional Rationale	Recommen-dation
			Monitor and local computer connection	
	Firewall Feature set	QOS support	Firewall capability that allows specific traffic to be prioritized (ie: health based traffic)	Recommended
	Firewall Feature set	Anti-spam, anti-malware, Antivirus, Web Filtering, etc	Firewall features that provide AV, span and malware protection at the firewall/gateway level. This combined with PC based protection is a layered security approach	Recommended
	Configuration	Firewall should block any known malicious traffic and generally any peer to peer traffic	Block all known Trojan outbound ports. List of known Trojan sites can be found online.	Strongly Recommended
	Configuration	By default block all inbound ports except those required for business critical services	It is best practice to block all inbound ports except those required for critical business functions. These might include: VPN ports for remote access, email, Web, SecureFTP, antivirus etc. Wherever feasible, inbound access should be enabled only from specific, trusted IP addresses or address ranges.	Strongly Recommended
Remote Access	Remote Access	Remote access to site resources should be managed via secure VPN tunnel (i.e., IPsec or SSL).	A firewall with this feature must be used if remote access is a requirement.	Required
Inter-site Access	Inter-site Access	Multiple sites sharing resources over the Public Internet or WAN, for example a Configuration 2 Hub and Spoke site, should have an IPsec VPN gateway tunnel connecting them or limit access to trusted IP addresses utilizing a secure protocol.	Standard IPSEC VPN connection to be implemented or a secure protocol (e.g. SSL, SSH) with cryptographically strong mutual authentication.	Required
Additional Recommendations – Related to Connectivity				
LAN	Wireless	If wireless router acts as a	WAP (Wireless Access	Required (if

Category		Requirements/ Considerations	Additional Rationale	Recommen-dation
	routers and WAP	firewall it should follow all recommendations listed in the firewall section. It should also be configured with Disabled SSID Broadcast WPA2-PSK Authentication Configured MAC Filtering	Point) should be configured with Disabled SSID Broadcast WPA2-PSK Authentication Configured MAC Filtering External Authentication Server like Radius Server, MS AD Server, etc.	wireless networking is used)
	PC	Personal Firewall	A software based personal firewall should be installed on all LAN connected PCs.	Required
	PC	O/S Patching	O/S Software patching should be maintained at current vendor release levels.	Required
	PC	O/S Patching service	A software update subscription will provide automated O/S patching delivery and may be offered by the O/S creator or reseller	Strongly recommended
Site Readiness	General User Security	Antivirus Software from a top-tier vendor	Antivirus software should be installed on every LAN connected PC. AV software should be set to update automatically and checked frequently.	Required
	Facilities	Uninterruptable Power Supply for site telecommunications equipment	To enable survivability of short-term power outages. Sizing requirements are site specific	Strongly recommended
	Facilities	Dedicated power outlet(s) for telecommunications equipment	To prevent interference from other non related appliances	Strongly recommended
	Facilities	Rack or sturdy shelving for Modem, Firewall appliance and LAN electronics	To prevent inadvertent movement of sensitive equipment and cabling	Recommended
	Facilities	Secure room for telecommunications equipment	To prevent tampering or inadvertent movement of sensitive equipment and cabling	Recommended

General Information Links

The following links provide additional general technical information related to the connectivity guidelines areas. The links are provided for informational purposes only and are not formal requirements of the eHealth Ontario EMR Connectivity Guidelines.

Resource Information	
List of all known Trojan ports	http://www.jlathamsite.com/dslr/suspectports.htm
Small office best practices	http://www.sans.org/reading_room/whitepapers/hsoffice/best_computer_security_practices_for_home_home_office_small_business_and_telecommuters_616?show=616.php&cat=hsoffice
Security Best practices	http://anti-trojan.org/index.html
Independent comparison of Antivirus Software	http://www.av-comparatives.org/
Belarc Advisor provides a list of windows based patches to be installed	http://www.belarc.com/free_download.html
For the MAC OS it is mandatory to run the MAC update process.	http://www.acosxhints.com/article.php?story=20090805215651603
In those cases where a static IP is not available from an ISP dyndns.org provides an alternative.	Dyndns.org name queries (http://www.dyndns.com/)
Personal Firewall Consideration	http://personal-firewall-software-review.toptenreviews.com/