	POLICY Number: 7311-25-011 Title: Wireless Access
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-007 Date Approved: August 1, 2014 Date Revised: Date Effective: August 1, 2014 Date Reaffirmed: Scope: SHR & Affiliates

OVERVIEW

This policy applies to all Saskatoon Health Region (SHR) Users and other persons acting on behalf of SHR who connect to SHR's systems or information via wireless access (i.e. using a mobile device to connect to SHR's computer network without wires).

Wireless access to SHR's network (sometimes referred to as WiFi) is implemented and maintained by SHR's Information Technology Services (ITS) department at all SHR owned and operated facilities, as well as at many SHR affiliate sites. Thus, for typical users (who utilize both SHR owned and managed mobile devices and wireless connections) all the technical requirements of this policy are automatically taken care of by merit of their using these established SHR IT standards, which will be automatically updated as technology and security standards change over time.

However, the contents of this policy also apply in the following situations:

- When SHR Users connect to SHR systems or information wirelessly from home or at another location (e.g. a third party clinic, the public library, a coffee shop, hotel) where wireless access is not implemented/managed by SHR ITS.
- When managers or business units wish to implement/expand additional SHR wireless network access.

This policy also supplements the provisions of SHR's User Account Policy, Security of Mobile Device Policy and Password Policy.

NOTE: A SHR User accessing SHR email, calendar, contacts etc. from smart phones (via Active Sync) or other mobile devices (via webmail) from data networks provided by a cell phone provider is **not** within the scope of this policy. For information on those types of connections, please refer to the SHR Policy *Security of Mobile Devices and Removable Media*.

DEFINITIONS

Mobile Device means a laptop computer or a pocket-sized computing device (a device typically having a display screen with touch input or a miniature keyboard that can store electronic data files and software). A mobile device includes but is not limited to: laptop computer, tablet computer, personal digital assistant (PDA), cellular phone, smart phone, and ultra-mobile PC (UMPC). *This includes home PCs and personal mobile devices used to access SHR's network, data, or applications.*

Guest Wireless means wireless internet access provided in good faith to patients/ residents and visitors at some SHR or SHR Affiliate facilities.

SHR User means a person with an active SHR User Account that allows access to the SHR computer network. A SHR User may include SHR employees, affiliate employees, physicians, other health care professionals, students, contractors, vendors and any other person who has been approved for an SHR User Account.

SHR Network means SHR's core/main computer network (and does not include the Physician's Internet wireless access or guest wireless access).

VPN (Virtual Private Network) means a software or hardware based way to connect directly to SHR's systems in a secure manner over a public network such as the Internet. All network traffic is encrypted, meaning that login credentials (e.g. username and password) and other information sent to and from a remote computer is not visible to eavesdroppers.

Wireless Access (sometimes referred to as WiFi) means accessing the SHR network directly without a network cable from a suitably-equipped Mobile Device.

1. PURPOSE

The purpose of this policy is to establish standards, for

- SHR's wireless (WiFi) network
- Types of devices that are permitted to connect directly to SHR's wireless network
- Equipment and connections used to wirelessly connect to the SHR network from a location other than a SHR facility. This can include but is not limited to, access from the following:
    - Connecting wirelessly from remote locations (for example, using a wireless router at home or at a third party clinic).
    - Third-party wireless internet service (also known as "WiFi hotspots") that SHR Users might be considering using to connect to SHR systems or information.
- Creation and management of wireless access points on SHR premises.
- Responsible and ethical use of SHR's guest wireless services by patients/residents and visitors.

2. PRINCIPLES

2.1. Wireless networking technologies are inherently less secure than wired networking technologies and require additional management, technical, and operational safeguards.

2.2 SHR has a responsibility to protect SHR's technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or loss of revenue resulting from any users utilizing wireless networking technology.

2.3 SHR Users are stewards of IT resources and are responsible for appropriate utilization of those resources in a manner consistent with SHR values and policies.

2.4 Patients/residents and visitors are expected to utilize guest wireless services provided to them in a manner that abides by all laws, all provincial and federal rules and regulations applicable to Internet use and all SHR policies. Further, excessive use of available guest wireless bandwidth is not acceptable.

3. POLICY

General

3.1 Only SHR owned, managed and/or supported devices are allowed to establish direct wireless connections to the SHR network.

3.2 Wireless access to SHR's network is a privilege, not a right.

3.2.1 Employment/contract relationship with SHR does not guarantee wireless access privileges.

3.2.2 Wireless access to SHR's network is not granted by default. It must be applied for (see procedure).

3.3 If you are utilizing an SHR owned and managed mobile device on an SHR managed wireless network, no action is required. In other situations, please ensure that all wireless equipment and connections used to access the SHR network adhere to the minimum requirements as defined in SHR's *Wireless Device Requirements for SHR Users* (see Appendix A). If doubt exists, please contact your Internet Service Provider (ISP) for technical advice and assistance.

3.4 All SHR User account activity via wireless network access is subject to the same user account responsibilities and restrictions as user activity via a direct connection to the SHR network. As such, SHR Users utilizing wireless access are responsible for knowing and complying with all associated SHR policies.

3.5 Patients/residents and visitors have access to guest wireless services that must be utilised responsibly, ethically and in accordance with SHR's Terms and Conditions (see Appendix B).

3.6 SHR reserves the right to turn off without notice any access port to the network that puts the organization's systems, data, users, and clients at risk or to prevent inappropriate use of resources.

Wireless Access Point Creation and Management

3.7 All access points that connect to the SHR network must be approved by the SHR'S Information Technology Services (ITS) department.

3.8 Non-sanctioned installation and/or use of unauthorized wireless equipment to connect to the SHR network is strictly prohibited. SHR will remove any equipment found meeting this criteria at the cost of the offender.

3.9 All wireless access points within SHR will be centrally managed by SHR ITS and will utilize encryption, strong authentication, and other security methods. SHR wireless security standards are subject to change over time as the associated threat landscape evolves.

Surveillance and Monitoring

3.10 Wireless access and/or connection to SHR's network may be monitored to record dates, times, duration of access, data types and volumes, etc., either for troubleshooting and maintenance purposes or in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties or improper use of network bandwidth.

3.11 An investigation may be pursued based on reports or suspicions of wrongdoing when concerns are raised to the Director of ITS regarding irresponsible and unethical use of IT resources, including guest wireless access.

Withdrawal of Wireless Access Privileges or Restricted Access

3.12 SHR Users are expected to adhere to the same security protocols while utilizing wireless access as they would if on the wired network. Failure to do so could result in immediate suspension of all network access privileges in order to protect SHR's information, systems, and IT infrastructure.

3.13 Any wireless connection used to conduct SHR business must be utilized responsibly and ethically. Failure to do so may result in immediate suspension of that user's account.

3.14 Guest wireless access must be utilized responsibly and ethically, and is subject to Terms and Conditions at each log in as defined by SHR and as amended from time to time.

3.14.1 SHR reserves the right to selectively block sites or deny/remove wireless access privileges/access points at the discretion of the respective Vice President in consultation with the Director, ITS.

- If in response to excessive bandwidth use, this decision is made by ITS.

3.14.2 For non SHR owned and managed facilities where SHR ITS manages guest wireless access, the Site Leader retains the authority to restrict/remove access.

4. ROLES AND RESPONSIBILITIES

4.1. All Staff

It is the responsibility of any SHR User connecting to the SHR network via wireless means from a location other than SHR, to ensure that all components of the wireless connection remain as secure as his or her network access within the office. SHR users must observe the following:

4.1.1 Use secure remote access procedures such as those discussed in SHR's Mobile Device policy. This will be enforced through encrypted strong passwords in accordance with SHR's password policy.

4.1.2 Never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

4.1.3 Ensure that non-SHR-managed wireless access within their control (e.g. using a wireless router at home to access SHR network, information, or information systems) adheres to the minimum requirements as defined in the Wireless Device Requirements (see Appendix A).

4.2 Managers

4.2.1 Ensure all new wireless access points and installation of wireless equipment in their area(s) of responsibility are approved, coordinated and managed though ITS.

4.2.2 Contact SHR ITS when they have (or suspect) security concerns exist with wireless access to SHR systems and data.

4.3 Information Technology Services

4.3.1 Implement, expand, and manage direct wireless access to SHR's network.

4.3.2 Advise SHR Users, managers, and other third parties about the policy expectations and technical standards established by this policy, including if/when/how these standards are applicable in a given situation. Any questions relating to this policy should be directed to the ITS Service Desk.

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

NON-COMPLIANCE/BREACH

Non-compliance with this policy will result in a review of the situation. Non-compliance may result in withdrawal of SHR wireless access privileges, suspension of that user's account, or disciplinary action up to and including termination of employment/contract relationship/privileges, particularly if the breach is intentional, major or relates to Personal Health Information.

Non-SHR user organizations and application providers will be responsible for implementing similar non-compliance policies for their employees.

6. REFERENCES

Portions adopted from the Saskatoon Health Information Network (SHIN) security framework, policy 8.7.7, Wireless Access.

Security of Mobile Devices and Removable Media

PROCEDURE Number: 7311-25-011 Title: Wireless Access	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-007 Date Approved: August 1, 2014 Date Revised: Date Effective: August 1, 2014 Date Reaffirmed: Scope: SHR & Affiliates

Note: Wireless Access (defined above, see **DEFINITIONS**) is **not** the same as a SHR User remotely accessing their SHR Outlook account (i.e. their SHR email, calendar, contacts, and tasks) from smart phones (via Active Sync) or other mobile devices (via webmail) from data networks provided by a cell phone provider.

For information and policy guidelines on those types of connections, please refer to the SHR policy Security of Mobile Devices and Removable Media.

1. Purpose

The purpose of this procedure is to establish the processes for applying for wireless access to the SHR network and extending existing wireless network coverage of this type.

2. Procedure

2.1. Applying for Wireless Access to the SHR Network

2.1.1 SHR Users who require wireless access for an SHR owned and managed device will have their Manager submit an ITS Work Order. This form is available on the "Forms" page of the ITS InfoNet.

2.1.2 ITS will add the user's device to the list of devices allowed to access the SHR network and contact the user with instructions regarding how to utilize this access.

2.2 Investigations:

2.2.1 An Investigation may be pursued based on reports or suspicions of wrongdoing when concerns are raised to Director, ITS regarding irresponsible and unethical use of IT resources, including guest wireless access.

- The principles of investigations (see SHR Fraud Procedure) will be followed.

2.3 Expanding SHR Wireless Network Coverage

If a SHR or SHR affiliate facility – or a specific area within such a facility – does not have adequate wireless network coverage, and a business unit feels wireless coverage would be of significant business or clinical benefit to their users:

2.3.1 The business unit or facility requests the expansion of SHR wireless coverage by submitting an ITS Work Order, including as many specifics as they can. This form is available on the "Forms" page of the ITS InfoNet.

2.3.2 An SHR ITS representative will do a site survey to determine if the proposed site/area is suitable for wireless. If there are no insurmountable technical issues, a cost estimate for implementing the requested coverage will be provided.

2.3.3 The coverage of the SHR wireless network is constantly expanding. However, unless project-specific funding has been acquired by ITS the sponsoring department or site is responsible for funding the associated costs of new/expanded wireless access.

2.4 Using Public Wireless

Be cautious when connecting a corporate device to <u>any</u> public Wi-Fi hotspot. Publicly-available wireless infrastructure that allows users to connect their mobile devices to the Internet via Wi-Fi hot spots etc. is typically unencrypted so that it is easier to connect to. However, the trade-off for this ease of use is that devices that use this public wireless are unprotected against malicious users as well as viruses. Here are some tips for securely using Wi-Fi networks when you're on the go doing work in hotels, airports, cafés and other public places.

2.4.1 Ensure that your mobile device is not configured to automatically connect to public Wi-Fi hotspots.

2.4.2 The most secure way to connect to the public Internet is to connect using a cellular hotspot from your smartphone. When available/viable, this connection method is more secure because cellular service providers use encryption when transferring data.

Caveats:

- Check your device's user manual or consult your cellular phone provide for advice on how to enable this feature.
- Unless you are streaming video or audio, or performing other actions that make high traffic demands on your smart phone's Internet connection, it is very unlikely you will exceed your monthly data limit. If you find SHR business use of your phone necessitates high data usage, you can avoid additional monthly charges by upgrading to an unlimited data plan.
- When you are travelling outside of Canada, do not use the data features of your smart phone or you will likely incur significant additional "data roaming" fees.

2.4.3 A reliable indicator for whether or not your Internet activity is secure or not is to look for the following indicators in your web browser: first, that the web page address begins with "https" (vs.

"http") and second that there is a "lock" icon present. (See Appendix A for screen captures that more clearly explain how to do this.) If both of those signs are visible in your web browser for both the login page and all subsequent web pages then you can consider your connection to be secure.

2.4.4 The security of other types of Internet connections that do not utilize a web browser like Internet Explorer is not so easy to determine. If in doubt, contact Information Technology Services for advice.

2.4.5 Refer to the SHR policy Security of Mobile Devices and Removable Media for additional safeguards that must be observed when conducting SHR business on mobile devices in public places. (Advice in this policy includes how to physically protect your mobile device from theft, and ensuring that other people are not watching over your shoulder when you are conducting SHR business.)

SHR's Wireless Device Requirements for SHR Users

Last updated: Jan 16, 2014

Corporate Wireless Device Requirements

All wireless infrastructure devices that connect to a Saskatoon Health Region (SHR) Network or provide access to SHR Internal* or Confidential* information must:

- Be installed, supported and maintained by an SHR ITS approved support team
- Use SHR approved authentication protocols and infrastructure
- Use SHR approved encryption protocols
- Maintain a hardware address (MAC Address) that can be registered and tracked
- Use a minimum security type of WPA2 (Wi-Fi Protected Access 2)
- Use an encryption type of AES (Advanced Encryption System)
- Use 802.1X Security known as a connection-based network access control
- Use Extensible Authentication Protocol Authentication via Secure Tunneling (EAP)
- Use Protected Extensible Authentication Protocol (PEAP)
- Use Authentication Key Management

Devices not capable of these requirements must be upgraded accordingly before wireless access to the SHR network is utilized. These requirements are available under any operating system as long as the network card installed in the device has the most up to date drivers. If updating the drivers is not possible then replacement of the card or the device will be required.

Isolated Wireless Device Requirements

All wireless infrastructure devices that provide access to Saskatoon Health Region (SHR) Internal* or Confidential* information must adhere to the Corporate Wireless Device Requirements specified above. Wireless devices that do not provide general network connectivity to the Saskatoon Health Region Network must:

- Be isolated from the corporate network (i.e. they must not provide corporate connectivity)
- Not interfere with corporate wireless access deployments

Home Wireless Device Requirements

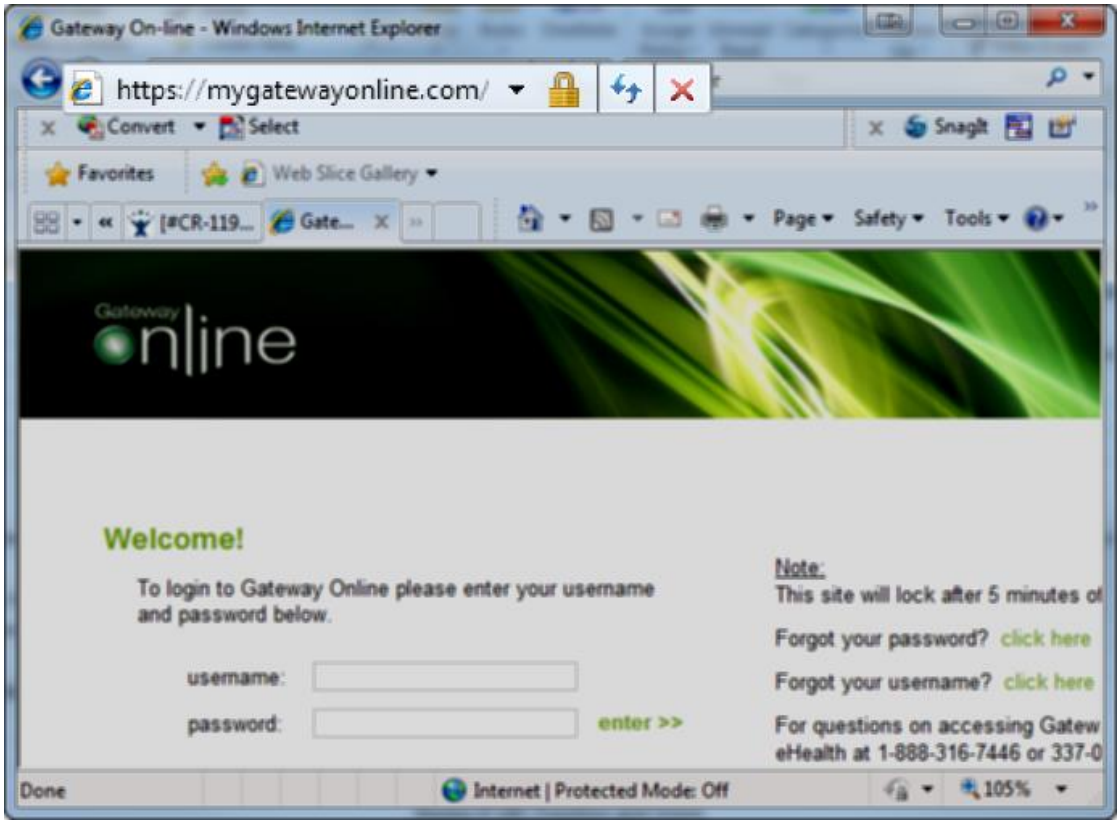
All home wireless infrastructure devices that provide direct access to a Saskatoon Health Region (SHR) Network, such as those behind Enterprise Teleworker or hardware VPN, must adhere to the following:

- Use a minimum security type of WPA (Wireless Protected Access)
- Enable WiFi Protected Access Pre-shared Key (WPA-PSK)
- When enabling WPA-PSK, configure a complex shared key (minimum 20 characters)
- Change the default SSID (Service Set Identifier) name
- Change the default username and password

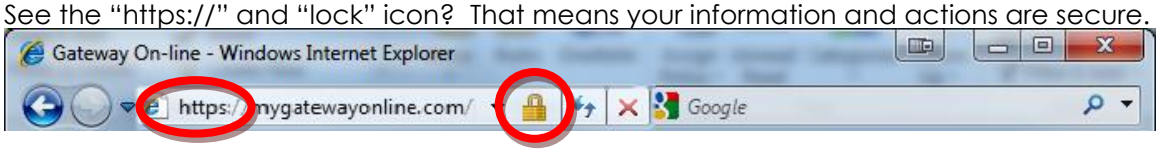
SHR ITS does not provide support for home wireless infrastructure devices or network connections. Users requiring technical assistance in meeting the above standards for their home wireless network should contact their home Internet Service Provider (ISP).

* *Definitions for what constitutes SHR Internal or Confidential information can be found in SHR policy 7311-75-010 Information Classification, Labelling and Handling.*

Example 1: A secure web page in Internet Explorer

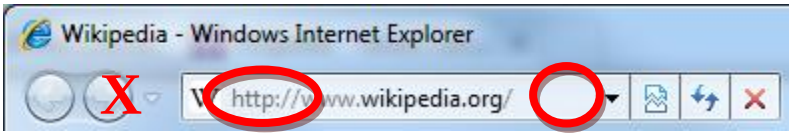


See the "https://" and "lock" icon? That means your information and actions are secure.



Example 2: An <u>insecure</u> web page

Notice how this web page address begins with just "http://" (i.e. the "s" in "https" that you would expect to see for secure web sites is missing), and that the lock icon is also missing? That means that your actions and keystrokes when accessing this web page are insecure, and may be viewable to others!



No lock icon!

NOTE: The location of the lock icon shown in these examples may vary from one web browser to another, but it should be present (either to the left or the right of the web page's address).

So, in summary, if…

- The lock icon is missing,
- The web page address begins with "http://" rather than "https://", or
- You receive security pop-up messages when visiting a web site

…be mindful that your actions (and the information you type) may be visible to others!

Appendix B

Terms and Conditions for Access to SHR Guest Wireless Services

Be advised that irresponsible, unethical, or illegal use of this wireless access, including unusually high consumption of this guest network's capacity may prompt an investigation which could result in discontinuation of service, restricted access, or criminal charges. By using this wireless access network, you agree to abide by all laws, all provincial and federal rules and regulations applicable to Internet use, and all Saskatoon Health Region Policies (including the policy governing guest wireless access) as published on SHR's public website.

Security Considerations

By providing wireless connectivity at facility as a guest service, the Saskatoon Health region offers no guarantees that any use of this wireless connection is in any way secure, or that your privacy can be protected. Wireless access is by nature an insecure medium. Do not transmit your credit card information, passwords and any other sensitive personal information while using a public wireless "hot spot". Users assume all associated risks, and agree to hold harmless the Saskatoon Health Region and its employees for any personal information (e.g. credit card) that is compromised, or for any damage caused to users' hardware or software due to electric surges, security issues or consequences caused by viruses or hacking.

Revised December 5, 2014