Saskatoon Health Region	**POLICY** Number: 7311-25-008 Title: Remote Access to Information Systems
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-004 Date Approved: July 31, 2014 Date Revised: Date Effective: August 1, 2014 Date Reaffirmed: Scope: SHR & Affiliates

DEFINITIONS

All staff means SHR employees, practitioner staff, professional staff, affiliates, contractors, vendors, students and volunteers.

IT GRC means the Information Technology Governance, Risk, and Compliance group within SHR's Information Technology Services (ITS) department. This group's roles and responsibilities are described in section 4.4, below.

Personal Health Information (PHI) means[1], with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;
(ii) information with respect to any health service provided to the individual;
(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
(iv) information that is collected:
    (A) in the course of providing health services to the individual; or
    (B) incidentally to the provision of health services to the individual;
    or
(v) registration information

Privacy Impact Assessment (PIA) means an evaluation process which allows those involved in the collection, use or disclosure of personal information to assess and evaluate privacy, confidentiality or security risks associated with these activities, and to develop measures intended to mitigate and, wherever possible, eliminate identified risks. This process is carried out under the direction of the SHR Privacy Office.

[1] HIPA Section 2 (m)

Remote Access means utilizing a public network such as the Internet to establish connectivity to SHR's network for the purpose of accessing SHR information or information systems.

Security Assessment means evaluating the controls currently in place against accidental or malicious disclosure, modification, or destruction of information and information systems and making recommendations for improvement. Information should be protected based on its value (sensitivity or criticality) and the risk of loss or compromise.

Saskatoon Health Region (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, physicians, other health care professionals, students, contractors, vendors and any other person who has been approved for an SHR User Account.

SHR User Account means a personal account consisting of an Active Directory username and a password that is granted user access privileges, as specified on the SHR User Account Application Form. Privileges may include access to shared files, email and/or systems/applications.

SHR User account activity means being logged onto the SHR network, by either direct/internal login or via remote access, using a computer or mobile computing device, in order to access SHR systems/applications and network resources.

Threat Risk Assessment means identifying the threats or vulnerabilities faced by a specific asset of value, determining the risk (i.e. likelihood and impact) of each threat, and developing protective and proactive measures to mitigate or eliminate these threats. This process is carried out under the direction of SHR's IT GRC group.

1. PURPOSE

The purpose of this policy is to set out the requirements for the granting of remote access to information systems under the custodianship of the SHR and to establish criteria and safeguards pertaining to remote access to information systems.

2. PRINCIPLES

SHR is required to establish clear accountability structures supported by appropriate systems, policies and procedures that will protect Personal Health Information accessed remotely through computer connections and any other electronic means from any unauthorized use, disclosure or modification as required under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act (HIPA)*, and any other applicable federal and/or provincial legislation.

3. POLICY

3.1 SHR shall grant remote access to information under its trusteeship only to authorized persons, and only for authorized purposes in accordance with this policy.

3.2 Remote Access Privileges - General

3.2.1 Remote access to information systems shall be granted on a limited basis to authorized persons who have a demonstrated need for access.

3.2.2 ITS will only consider requests that have been pre-approved. The party authorized to approve (i.e. verify the operational need for) remote access requests varies depending upon the affiliation of the person or organization requesting access (see 3.3 below).

3.2.3 Remote access to the SHR network and resources will only be permitted providing that authorized SHR Users are specifically authenticated (no generic or anonymous access accounts), data is encrypted across the network (from client workstation to SHR network), and privileges are restricted to the appropriate information and systems. Refer to *Appendix A: Acceptance Criteria for Remote Access Connections*.

3.2.4 All SHR User account activity via remote 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 remote access are responsible for knowing and complying with all associated SHR policies.

3.2.5 SHR Privacy and SHR ITS reserve the right to reject requests or to remove access if privacy or security related concerns are not addressed to their satisfaction.

3.3 Approval

3.3.1 **SHR Staff:** Remote access requests shall be pre-approved and submitted to ITS by an employee's Director or appointed designate.

3.3.2 **U of S staff and residents:** Remote access requests shall be pre-approved and submitted to ITS by the applicant's designated department/division head or administrator.

3.3.3 **Contracted Physicians:** remote access requests shall be pre-approved and submitted to ITS by the Department Head or Practitioner Staff Affairs.

3.3.3.1 Remote access to the SHR network and resources will only be permitted to contracted physicians that have adequate security precautions in place, as determined by ITS. Refer to *SHR Local Workstation Security Guidelines*.

3.3.4 **"Business to Business" (third party access)**

3.3.4.1 Approval

Requests for "Business To Business" access (i.e., connection between a distinct network infrastructure and that of SHR) shall be submitted, in writing, to ITS via the IT Change Management group. Requests shall include a copy of the respective third party's non-compliance policy, including the disciplinary actions and penalties that their employees or contractors would be subject to should they breach the policies of their organization or those of the organization's

clients. Such connections shall require the approval of the Director, Information Technology Services (or designate).

3.3.4.2 Privacy Impact Assessment (PIA)

The need for a PIA shall be determined by SHR's Privacy Office. In the event that a PIA is required, it shall be carried out under the direction of the SHR Privacy Officer.

3.3.4.3 Threat Risk Assessment (TRA)

For each application, a Threat Risk Assessment followed up with a Security Assessment will also be carried out under the direction of SHR's IT GRC group.

3.3.4.4 A Privacy Impact Assessment and a Threat Risk Assessment are required **prior to** granting access to third party organizations/individuals. Any decision with respect to the application for remote access shall be subject to the findings and recommendations of these assessments.

3.3.4.5 Authorization of remote access shall be deemed sufficient to acquire remote access to SHR's network and the data and resources typically available via a SHR User account.

3.3.4.6 Data sharing or creation, especially that requiring access to specific information systems, shall require the negotiation of additional agreements. These agreements shall contain terms with respect to route of access, and information capture, creation, maintenance, retention, disposal and/or destruction of shared or captured information.

3.3.5 **Vendors/Contractors**

3.3.5.1 Approval

Remote access requests must be pre-approved and submitted to ITS by a SHR manager. Requests shall include a copy of the respective vendor's/contractor's non-compliance policy, including the disciplinary actions and penalties that their employees or contractors would be subject to should they breach the policies of their organization or those of the organization's clients.

3.3.5.2 In the event that a vendor/contractor requires remote access to SHR network applications for the purposes of providing system and/or application support, SHR shall enter into a contractual relationship. The contract shall clearly outline the terms and conditions for the granting of remote access privileges and clearly indicate the vendor's/contractor's confidentiality obligations regarding SHR information and information systems.

3.3.5.3 Threat Risk Assessment (TRA)

For each vendor/contractor, a Threat Risk Assessment will be carried out under the direction of SHR's IT GRC group.

3.3.5.4 Any decision with respect to the application for remote access shall be subject to the findings and recommendations of this assessment.

3.4 Access Methods

Secure network connections shall conform to SHR standards established by IT. SHR/IT reserves the right to refuse connections and connection methods that it deems insecure or otherwise not in conformance with SHR's established standards.

3.5 Costs

Any costs incurred by SHR in the provision of Remote Access shall be payable by the applicant/department/unit or sector. Costs, as determined by fee schedules established by SHR, may include expenses for computer hardware, software requirements, or costs of ongoing technical support.

3.6 Training

3.6.1 The applicant shall be required to undergo training or demonstrate competence for the application(s) to which he/she has requested remote access. Training shall be provided by SHR. The applicant shall be responsible to contact the appropriate application "owner(s)" and attend all required training sessions before the remote connection is established.

3.6.2 The applicant shall be required to undergo security and privacy awareness training as provided by SHR prior to gaining access to remote systems.

3.7 Surveillance and Monitoring

3.7.1 SHR reserves the right to monitor and audit any and all access to information and information systems under the trusteeship of SHR. The surveillance and auditing may include: periodic reviews, random audits, and pattern recognition of individual usage of personal health information to ensure compliance with the protection of privacy guidelines.

3.7.2 SHR's Security Office and Privacy Office may be required to provide audit and log reports of access to information under the trusteeship of SHR in support of access requests. The reports will include: who accessed the information, when the access was done and what information was accessed.

3.7.3 SHR reserves the right to audit any device used for remote access to verify that they are in compliance with SHR IT security standards.

3.8 Withdrawal of Remote Access Privileges

3.8.1 Inappropriate access, use or disclosure of information under the trusteeship of SHR shall result in the immediate withdrawal of remote access privileges and the filing of an IT Security Incident Report with the SHR's IT GRC group and Privacy Office in accordance with SHR Policy: IT Security Incident Management.

3.8.2 No SHR User shall have remote access while on a Leave of Absence (LOA) unless explicitly requested by the appropriate authorizing party. The authorizing party for remote access is responsible for informing ITS Security **in writing** in advance of a LOA so that remote access for the respective user can be suspended or extended.

3.8.3 Privileges will also be withdrawn in the event that computer infrastructure for the remote access fails to meet SHR's IT security standards. Refer to *Appendix A: Acceptance Criteria for Remote Access Connections* and *SHR Local Workstation Security Guidelines.*

3.9 Destruction and Disposal of Information

3.9.1 SHR Users and the organizations granted remote access shall destroy, thoroughly delete or erase, securely shred or otherwise securely dispose of all copies of personal health information or other confidential information after their job function has been changed, their employment has been terminated, the purpose for which the information was originally acquired has expired, or the relationship of the SHR User or their employer to SHR has otherwise been altered so that retention of this information is no longer required. Without limiting the general nature of the preceding sentence, SHR Users shall not dispose of any documents containing confidential information into the trash without securely shredding them first.

3.9.2 If the SHR User is unable or unwilling to perform this secure destruction or disposal of information, the user's manager or employer shall be responsible for doing so.

3.9.3 SHR reserves the right to audit any device used for remote access in order to verify that all personal health information or other confidential or restricted information has been removed.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users Granted Remote Access

4.1.1 SHR Users granted remote access to information shall:

- Comply with all applicable contracts or agreements
- Protect the confidentiality and privacy of information in accordance with SHR policy *Confidentiality - Health Information*
- Remotely access and use SHR information and information systems responsibly and for purposes authorized within the scope of their duties with (or on behalf of) the SHR
- Be responsible and accountable for all activities conducted on SHR systems/applications using remote access
- Take all reasonable steps to prevent unauthorized access to:
    - the computer or other device by which they remotely access the SHR's computer systems; and
    - any and all paper documents or electronic documents (such as disks) containing any confidential information that they may generate, create and/or print-off.
- Immediately report all unauthorized use (or suspicions of unauthorized use) to their manager
- Maintain the integrity, accuracy, and privacy of personal health information

- Maintain the computer, hardware, and network infrastructure they use for remote access in compliance with SHR's IT security standards, both at the time remote access is granted and as these standards may be amended from time to time.
- Review and understand their personal responsibility and liability when it comes to unauthorized use, disclosure or modification of information relative to *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act (HIPA)*, and any other applicable federal and/or provincial legislation

4.1.2 SHR Users shall not use, modify, or disclose personal health information to non-authorized persons unless it is done in accordance with *The Health Information Protection Act* and SHR's privacy and/or security Policies.

4.1.3 SHR Users granted remote access capability shall prevent unauthorized access to SHR systems/applications; they shall not allow other, unauthorized parties to utilize their access, either by utilizing their credentials or by otherwise sharing or delegating the access granted to specific computer workstations. Any remote connection or method not authorized through proper channels is prohibited.

4.1.4 The applicant/department/unit or sector requiring remote access shall pay any costs incurred by SHR in the provision of remote access, see section 3.3, "Costs".

4.2 Managers

4.2.1 Vet, approve and submit requests for remote access in cases where they deem it necessary for SHR operational reasons.

4.2.2 Enforce the provisions of this policy to the best of their knowledge and ability

4.2.3 Immediately call the ITS Service Desk at 655-8200 in situations where they know of (or suspect) misuse, unauthorized use, or other security risks to SHR systems or applications.

4.3 SHR Privacy Office

4.3.1 Determine whether a remote access request requires a PIA.

4.3.2 Oversee the execution of PIAs.

4.3.3 Reserve the right to refuse a remote access request if privacy concerns are not addressed to their satisfaction.

4.3.4 Reserve the right to monitor and audit any and all access to personal health information.

4.3.4 Provide or coordinate and oversee the retrieval and provision of audit and log reports of access to personal health information in support of access requests.

4.4 SHR IT Governance, Risk, and Compliance (GRC)

4.4.1 Determine whether a remote access request requires a Threat Risk Assessment and Security Assessment.

4.4.2 Direct and oversee the execution of a Threat Risk Assessments and Security Assessments.

4.4.3 Reserve the right to refuse a remote access request if security concerns are not addressed to their satisfaction.

4.4.4 Reserve the right to monitor and audit any and all access to personal health information.

4.4.5 Provide or coordinates and oversee the retrieval and provision of audit and log reports of access to personal health information in support of access requests.

4.4.6 Protect electronic information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction through the implementation, oversight, and monitoring of appropriate administrative, physical, and technical safeguards.

4.4.7 Provide (or coordinate the provision of) associated expertise to other SHR business units, as well as conduct, oversee, or contribute to investigations of IT security incidents; this includes, but is not limited to, actual or suspected violations of regional IT policies and IT standards.

5. POLICY MANAGEMENT

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

6. NON-COMPLIANCE/BREACH

Non-compliance to this policy by SHR employees or employees of contractors providing services to SHR may lead to disciplinary action including termination of employment/ privileges and/or contract relationship if breach is intentional, major or relates to Personal Health Information. SHR User Organizations and Application Providers will be responsible for implementing similar non-compliance policies for their employees. Violations may also result in significant legal fines and/or imprisonment[2] for the offending individual(s).

7. REFERENCES

Adopted from the eHealth Saskatchewan Security Policy Framework, section 11.7.2, Granting of Remote Access to Information Systems.

SHR User Account Policy

SHR's *Local Workstation Security Guidelines*

Setup of Laptops Provided by a Third Party

[2] HIPA Section 64(2)(a)

PROCEDURE Number: 7311-25-008 Title: Remote Access to Information Systems	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: Date Approved: July 31, 2014 Date Revised: Date Effective: August 1, 2014 Date Reaffirmed: Scope: SHR & Affiliates

PROCEDURE

1. PURPOSE

The purpose of this procedure is to establish the process for applying for remote access privileges.

2. Procedure

2.1 SHR Staff, U of S Staff and Residents, and Contracted Physicians

The person requiring remote access identifies their need to the appropriate authorizing party (see policy section 3.3).

2.1.1 The authorizing party evaluates whether the request meets the criteria set out in *Appendix A - Acceptance Criteria for Remote Access Connections* and, if a laptop is to be used, *Appendix B - Acceptance Criteria for Laptops Connecting to the SHR Network*.

2.1.2 If the applicant has a valid need, the authorizing party asks the applicant to read and sign a copy *SHR's Remote Access Agreement (Appendix C)*.

- A signed *Remote Access Agreement* (see Appendix C) is required from every applicant for remote access.

2.1.3 The authorizing party forwards the applicant's signed Remote Access Agreement, along with their own authorization of the request, to ITS for evaluation and processing.

2.2 "Business to Business" (third party access)

2.2.1 **Privacy Impact Assessment (PIA)**
The need for a PIA shall be determined by SHR's Privacy Office. In the event that a PIA is required, it shall be carried out under the direction of the SHR Privacy Officer.

2.2.2 **Threat Risk Assessment (TRA)**
For each application, a Threat Risk Assessment followed up with a Security Assessment will also be carried out under the direction of SHR's IT GRC group.

2.2.3 A Privacy Impact Assessment and a Threat Risk Assessment are required **prior** to granting access to third party organizations/individuals. Any decision with respect to the application for remote access shall be subject to the findings and recommendations of these assessments.

2.2.4 A Service Level Agreement shall outline the level of information technology support to be provided by SHR. This service level agreement shall apply to network connectivity only – it shall not apply to computer hardware or application support.

2.3 Vendor Support

2.3.1 In the event that a vendor requires remote access to SHR network applications that contain personal health information for the purposes of providing system and/or application support, SHR shall enter into a contractual relationship with the vendor. The contract shall clearly outline the terms and conditions for the granting of remote access privileges and clearly indicate the vendor's confidentiality obligations regarding SHR information and information systems.

2.3.2 **Threat Risk Assessment (TRA)**
For each vendor, a Threat Risk Assessment will be carried out under the direction of SHR's IT GRC group.

2.3.3 Any decision with respect to the application for remote access shall be subject to the findings and recommendations of this assessment.

2.3.4 A signed Remote Access Agreement (see Appendix C) is required from every applicant for remote access.

3. PROCEDURE MANAGEMENT

The management of this procedure including procedures education, monitoring, implementation and amendment is the responsibility of the Director, Information technology Services.

4. NON-COMPLIANCE/BREACH

Non-compliance with this procedure will result in remote access privileges being denied.

Appendix A

Acceptance Criteria for Remote Access Connections

Remote Access shall be approved subject to the following criteria:

1. The applicant is an Authorized Person (i.e. an SHR employee, affiliate employee, physician, other health care professional, student, contractor, vendor and any other person who has been approved for an SHR User Account).

2. The applicant requires access to information contained in the network application in order to effectively carry out his or her responsibilities with the Saskatoon Health Region for one or more of the following authorized purposes:
   - to provide care and treatment;
   - to determine or verify eligibility for a health service;
   - to conduct investigations of health service providers and staff;
   - health service provider education;
   - research conducted under specific reviews and conditions;
   - internal management (i.e. planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, processing health service payments and human resource management);
   - remote troubleshooting and support of information systems and IT infrastructure;
   - Regional health system and public health surveillance.

3. The applicant signs and agrees to adhere to the required Remote Access Agreement.

4. The applicant agrees to Saskatoon Health Region conducting a Privacy Impact Assessment (if deemed necessary).

5. The applicant agrees to Saskatoon Health Region reserving the right to conduct periodic review and audits of Remote Access usage.

6. The applicant agrees to equip the computer(s) remotely connected to the Saskatoon Health Region network with up-to-date virus/spyware detection software, a desktop firewall, and an up-to-date operating system. *These restrictions apply to both Microsoft Windows and Apple Mac OS devices.*

   The need for firewalls and virus/spyware detection software does not apply to mobile devices (e.g. iPads) or smart phones (e.g. iPhones) for which these controls are not available; however, the operating systems on these devices must still be kept up to date, and the use of devices which are "jailbroken" – on which users have broken and circumvented built-in operating system and other device-specific security controls – is strictly forbidden.

If in doubt whether a device meets SHR's IT security standards, users should contact the ITS Service Desk for advice and assistance.

Appendix B

Acceptance Criteria for Laptops Connecting to the SHR Network

Criteria for connecting non-desktop systems to the SHR network falls into 3 categories:

1. Laptop provided by SHR
2. Laptop provided by a consultant working on contract.
3. Laptop provided by users other than above, requiring temporary access to the internet.

Laptop provided by SHR to an employee, consultant, or other SHR User

All laptops are initially configured by SHR ITS to ensure the following security requirements are met:

1. All serial numbers and laptop system identifiers are logged into an asset management system.
2. Corporate standard operating systems are installed, and the system configured to receive regular, SHR-tested updates for system patches.
3. SHR's standard anti-virus software is installed and set to receive regular virus signature file updates.
4. A suite of office productivity applications are installed and working.
5. Any additional software that is required by the employee to perform their job function (e.g. Visio, Microsoft Project) is also installed and functioning.
6. All licenses for software products installed are identified and tracked within an asset management system.
7. A personal firewall (e.g. Windows firewall) is on (enable) and configured to restrict access to incoming connections.
8. Systems awareness and usage training is to be provided to the user prior to or at the time of receiving the laptop system.

Laptop provided by a consultant working on contract

At times it is necessary for consultants who provide services to SHR on a short or long term basis to connect to the SHR domain and network. When this need arises, the following procedures will be followed:

1. Account authorization forms must be completed indicating that network access is required, signed by a supervisor.
2. Laptop operating systems are checked and verified that they are able to be remotely scanned by internal SHR security systems to ensure they are up to date with the latest patches. e.g. Windows 7, Windows Vista, Windows XP Pro, variants of Linux.
3. Laptop operating systems are checked and verified to ensure that they can easily connect to the SHR network without modification to the laptop.
4. *Laptops must be re-checked if they are away from the network for more than 90 day.s*

NOTE: For steps 5-10, fill out a copy of the SHR form *Setups of Laptops Provided by a Third Party*, available on the "Forms" page of the ITS InfoNet.

5. Laptop operating systems are checked and verified that they are up to date with the latest operating system patches and fixes.
6. Laptop operating systems are checked and verified that they are setup to receive regular updates for system patches. If the system is not configured to receive regular updates, process documentation will be provided to the consultant.
7. Laptop is checked to ensure that an enterprise version of anti-virus software is installed and set to receive regular virus signature file updates. If the system is not configured with an anti-virus software package, process documentation will be provided to the consultant.
8. Laptop is checked for software that may have an adverse affect on the SHR network, such as peer-2-peer or various network hacking tools like packet sniffers.
9. Laptop is checked to ensure that a personal firewall is installed and configured to restrict access to incoming connections.
10. If the laptop completely passes the security scan, the SHR User's laptop can connect directly to the internal network and a SHR profile will be created allowing them to receive network drive mappings and email.
11. If account authorization for remote access to the SHR network is approved, the necessary client certificates, internet links and Citrix client software will be installed allowing Secure Remote Access (SRA) to the SHR network.

If the laptop does not completely pass the above security scan, the user's laptop must not be plugged into SHR's network until the above conditions can be met.

Upon the end of the Consultant's term, the laptop is to be returned to SHR for inspection.

Laptop provided by users other than above that require temporary Internet access

Restricted ports in meeting rooms will be provided for laptop systems that are not provided by SHR or consultants providing services to SHR. These restricted ports will place these systems within a restricted area of the SHR network that only has direct access to the internet.

Appendix C

Remote Access Agreement

I have requested remote access to certain Saskatoon Regional Health Authority (SHR) computer applications. I understand that additional privacy and security risks are associated with such remote access. I also understand that the data I remotely access (the "Data") may include highly sensitive personal health information.

Therefore, in consideration of being granted remote access to the Data and SHR's computer systems, I hereby agree that:

1. I will only remotely access SHR's computer systems in accordance with applicable SHR information technology policies (including any specific remote access policies that may be established by SHR). I understand that such policies may be supplemented or amended from time to time by the SHR (including for the purpose of complying with any new or existing privacy laws) and that my continued remote access to SHR's computer systems signifies my acceptance of such supplements or amendments. If I am unable or unwilling to comply with any such supplements or amendments, my sole remedy is to cease remotely accessing SHR's computer systems.

2. Without limiting the general effect of section 1, I understand that SHR reserves the right to evaluate the computer systems (including hardware, software and other network components) that are used to access SHR's computer systems and data related to my particular situation (taking into account, among other things, the types of applications I am permitted to access). I agree to comply with such requirements, as they may be amended from time to time. I agree that SHR reserves the right to revoke my access in the event that the computer systems I am using for remote access fail to meet SHR's IT security standards.

3. I will take all reasonable steps to prevent unauthorized access to:
   (a) the computer (or other device) by which I may remotely access SHR's computer systems; and
   (b) any and all paper or electronic documents containing Data that I may generate, create and/or print-off.

   This shall include, but not be limited to:
   - Keeping strictly confidential the login ID*, password and all other information that enables such access.
     * *The log in ID is the electronic means of personally identifying an individual. This log in ID will be used to hold individuals accountable, as required by HIPA, for any and all access to personal health information.*
   - Practising good workstation security measures such as using screen savers and positioning of screens away from public view.
   - Disposal of printed personal health information by confidential shredding.

4. I will only remotely access SHR's computer systems as necessary for purposes within the scope of my professional duties with the Saskatoon Health Region.

5. Unless otherwise required by law or professional ethical obligations, I will thoroughly delete any Data from the computer or other device by which I remotely access SHR's computer systems as soon as the Data is no longer needed for the purposes for which it was accessed. Further, if I generate, create or print-off any paper documents or electronic documents

containing any Data, I agree to thoroughly destroy or erase such documents when they are no longer needed.

6. I will protect the security and confidentiality of any Data under my control (including, for greater certainty, paper or electronic documents containing Data) to at least the same standard as I protect my most sensitive confidential patient information.

7. I agree that the obligations contained in this letter are intended to be complimentary to any obligations I may have pursuant to:

   (a) any other agreement(s) between myself and SHR;
   (b) applicable SHR policies;
   (c) applicable laws; or
   (d) my professional ethical obligations.

   To the extent of any inconsistency between such obligations, the obligations imposing the highest security and confidentiality standard shall govern.

8. I agree that my obligations pursuant to this agreement will continue after any termination of this agreement or my affiliation with SHR. I further agree to notify the SHR to inactivate my remote access immediately upon any such termination.

9. I agree to equip the computer(s) remotely connected to the SHR network with up-to-date virus and spyware detection software, a desktop firewall, and an up-to-date operating system. Apple iOS (iPad, iPhone) and Android devices must have up-to-date operating systems and must not be "jailbroken" (which allows circumvention of existing system controls).

10. I agree and accept that my access to patient information will be tracked. I acknowledge that my user name will identify myself as the individual accessing data to which remote access has been granted.

11. I understand that an audit log of access to personal health information will be provided to a patient/client upon request.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above. I further agree that any breach of this agreement may be enforced by injunctive relief in addition to any other remedy available to SHR.

REQUESTER

Signature	Date
Printed Name	Email Address

AUTHORIZER

Signature	Date
Printed Name	Email Address

Remote access needs to be authorized by (as appropriate) a user's Director, Department, or Division Head. Once signed by both the requester and authorizer, this form (both pages) should be scanned and emailed to itssecurity@saskatoonhealthregion.ca