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