
 PRIMARY HEALTH CARE OPERATIONAL GUIDELINE	Operational Guideline: <i>Remote Access to Electronic Medical Record</i>	Guideline Number: <i>PCOG #26</i>
	Approved By: <i>Community Primary Care Council</i>	Pages: <i>1 of 4</i>
	Approval Date: <i>REVISED January 12, 2016</i>	Supercedes: <i>February 12, 2014</i>

1. INTENT

- A key objective in managing patient information is to provide timely and secure access to all relevant aspects of a patient's health history in a manner that respects patient rights to privacy and confidentiality. To meet this commitment it is necessary to establish a coordinated and uniform Operating Guideline on Remote Access within the Primary Health Care Program to assure the privacy and security of patient Personal Health Information contained in the Electronic Medical Record (EMR).
- To ensure Personal Health Information is protected during its collection, use, disclosure, storage, and destruction in accordance with the provisions of the *Personal Health Information Act (PHIA)*. All WRHA Regional PHIA (#10.40) and Information Technology (#70.030) Policies are to be adhered to and followed <http://home.wrha.mb.ca/corp/policy/policy.php>
- This guideline applies to all persons who are authorized to gain Remote Access to the EMR containing Personal Health Information via the use of a non-Manitoba eHealth managed computer within the WRHA Primary Care Direct Operated Clinics, Family Medicine Teaching Clinics, and Quick Care Clinics. Pending further evolution of Remote Access technology and related Regional Policies, this guideline will be revised accordingly as needed to reflect current state and practice.

2. DEFINITIONS

- **Authorized User** is a User who is authorized pursuant to this guideline to gain Remote Access to EMR.
- **Electronic Medical Record (EMR)** is a secure electronic record of a patient's health care history including, but not limited to, appointment history, medications, laboratory results, diagnostic images and encounter records maintained in the Electronic Medical Records software.
- **Manitoba eHealth Managed Computer** is a computing device equipped and configured to meet Manitoba eHealth security requirements and then continuously managed by Manitoba eHealth to ensure its technical safeguards remain current.
- **Manitoba eHealth Network** is the closed private data transport network operated by Manitoba eHealth that connects all major WRHA sites and many other Health Authority sites.
- **Remote Access** is the process of accessing WRHA and Manitoba eHealth networks by using third party data communication connections that are not controlled by Manitoba eHealth.
- **Security Token** is a small physical device (i.e. fob) or software application, as prescribed by Manitoba eHealth, which is used to authorize access to the EMR utilizing two-factor authentication.
- **Two-Factor Authentication** is the process by which an information system uses two different methods to verify the identity of a User wishing to access it.


 PRIMARY HEALTH CARE OPERATIONAL GUIDELINE	Operational Guideline: <i>Remote Access to Electronic Medical Record</i>	Guideline Number: <i>PCOG #26</i>
	Approved By: <i>Community Primary Care Council</i>	Pages: <i>2 of 4</i>
	Approval Date: <i>REVISED January 12, 2016</i>	Supercedes: <i>February 12, 2014</i>

- **User** is any person (employee, associate, or contractor) authorized to access the Manitoba eHealth network.

3. GUIDELINE

This guideline defines requirements and procedures for allowing an Authorized User to gain Remote Access to the EMR, and thereby to Personal Health Information, by means of third party data communications connection to the Manitoba eHealth Network.

- 3.1 Remote Access to EMR shall be authorized and granted on a limited basis to a User who has a demonstrated need for such access. All requests for remote access to the EMR via the use of a Security Token must meet one the following criteria in order to be eligible:
 - Be a physician or resident who is required to deliver service for the Region After-Hours and as a result, requires access to the patient's health record in EMR to do so
 - Be a Primary Care Clinician who delivers service for the Region off-site or After Hours with no access to a Manitoba eHealth managed computer
- 3.2 All requests for Remote Access must be approved and signed off by the appropriate Site Director responsible for Primary Care or in the event of requests from Centralized Services, by the Primary Care Program Director. The completed, signed, and approved Remote Access Service (RAS) Request Form (Appendix A) shall be directed to the Manitoba eHealth Service Desk for processing.
- 3.3 An Authorized Users clinical requirement for Remote Access privileges will be reviewed on an annual basis by the Site Director responsible for Primary Care/Program Director (or designate). An Authorized User who no longer requires Remote Access privileges will have their Remote Access privileges cancelled and account removed.
- 3.4 All associated annual costs will be the responsibility of the appropriate Community Area Primary Care, Family Medicine Teaching Clinic or Centralized Program Operating Budget. There is an annual fee payable for every Security Token assigned. For current pricing contact Manitoba eHealth Service Desk at 204-940-8500 or servicedesk@manitoba-ehealth.ca.
- 3.5 Remote Access connections to Clinical Information Systems require the use of two factor authentication. Each Security Token is assigned to a single User – this is the first level of security. Every User will also have a unique User ID and password – this is the second level of security. Remote Access Security Tokens provided by Manitoba eHealth are personally assigned, and shall not be shared with or loaned to any other person.
- 3.6 It is recommended that Users maintain the standard Manitoba eHealth supported version of Internet Explorer on their non-Manitoba eHealth managed computers

 PRIMARY HEALTH CARE OPERATIONAL GUIDELINE	Operational Guideline: <i>Remote Access to Electronic Medical Record</i>	Guideline Number: <i>PCOG #26</i>
	Approved By: <i>Community Primary Care Council</i>	Pages: <i>3 of 4</i>
	Approval Date: <i>REVISED January 12, 2016</i>	Supercedes: <i>February 12, 2014</i>

that run Accuro EMR via Citrix – PHAN connection. Installation of some newer versions may in certain cases prevent Users from being able to launch the Accuro Application.

3.7 During a Remote Access Session, an Authorized User shall:

- Comply with all applicable contracts and agreements
- Comply with all applicable WRHA Policies including this Operating Guideline
- Protect the confidentiality and privacy of Personal Health Information
- Use the Personal Health Information responsibly and appropriately
- Maintain the integrity and accuracy of the Personal Health Information
- Adhere to recognized best practices for safe and secure computing
- Refrain from the printing of any Personal Health Information

3.8 When an Authorized User no longer requires Remote Access (whether as a result of a job change, no longer meeting the requirements for Remote Access, or otherwise), the Site Director responsible for Primary Care/Program Director (or designate) shall immediately notify Manitoba eHealth to have the Remote Access privileges for that individual revoked.

3.9 Users of Security Tokens assigned to them, will be assessed a replacement fee for lost or damaged Security Tokens. In the event of a lost or damaged Security Token, the respective Site Director responsible for Primary Care/Program Director (or designate) must be notified immediately.

4. **SOURCE/REFERENCES**


- Draft WRHA Regional Policy “Remote Access to Information Systems maintaining Personal Health Information”, December 19, 2011
- EMR Implementation Committee, Discussion/Consensus at July 23, September 17, October 15, 2013 meetings. Input from CSIS, PCIS, MB eHealth, Community Area Directors, CAO, Family Medicine, and Primary Care Program
- Consultation with Landis Esposito, WRHA - Chief Privacy Officer (2013)
- Consultation with Jennifer Glen, MB eHealth - Director & Solution Information Officer, Community & LTC (2013)
- WRHA PHIA Policies, <http://home.wrha.mb.ca/corp/policy/policy.php>
- Consultation with Christian Becker, Administrative and Process Development Specialist, Family Medicine Teaching Clinics (December 2015)
- WRHA Regional Policy #70.030.010 – Information Technology (IT) Security, June 2011
- WRHA Regional Policy #70.030.020 – Wireless Local Area Network Technology Security, January 2012

5. **PRIMARY AUTHOR**

- Kevin Mozdzen – Primary Health Care, Program Specialist
- Jo-Anne Kilgour – Primary Health Care, Program Specialist

6. **ALTERNATE CONTACT**

- Jeanette Edwards - Regional Director, WRHA Primary Health Care and Chronic Disease
- Christian Becker – Administrative and Process Improvement Specialist, Primary Health Care

 Winnipeg Regional Health Authority Office régional de la santé de Winnipeg Caring for Health À l'écoute de notre santé	Operational Guideline: <i>Remote Access to Electronic Medical Record</i>	Guideline Number: <i>PCOG #26</i>
	Approved By: <i>Community Primary Care Council</i>	Pages: <i>4 of 4</i>
	Approval Date: <i>REVISED January 12, 2016</i>	Supercedes: <i>February 12, 2014</i>

7. APPENDICES

- Appendix A – Remote Access Service (RAS) Request Form
- Appendix B – Application Viewer, User Guide

SCOPE: Applicable to all WRHA Primary Care Direct Operated Clinics, Family Medicine Teaching Clinics, and Quick Care Clinics