Shared health Soins communs Manitoba

Public Health Information Management System

MEMO

Date: July 5, 2021

To: All PHIMS Authorized Account Sponsors and Authorized Account Requestors

From: Lynda Tjaden, Executive Director, Population and Public Health, Manitoba Health and Seniors Care;

Kathy Koschik, Manager, Public Health Systems, Digital Health, Shared Health;

CC: Gillian Brennan, Executive Director, Digital Health Shared Health;

Sandeep Anand, Director, Home and Community Care, Digital Health Shared Health

Re: **Responsibilities of PHIMS Authorized Account Sponsors and Authorized Account Requestors, and Privacy Reminders**

As Authorized Account Sponsors and Authorized Account Requestors, you have important responsibilities to ensures personal health information (PHI) in PHIMS is kept safe.

Your attention in this matter is crucial to ensure Authorized Users comply with the proper use of PHIMS under the terms and conditions identified in the PHIMS Information Sharing Agreement, and the PHIMS Electronic Terms of Use.

Responsibilities for Authorized Account Sponsors and Authorized Account Requestors

Role	Responsibilities
Authorized Account Sponsor	• Authorizes users at the site to access PHIMS. • Accountable for user account requests **(Add/Modify/Terminate).** • Accountable for user activity in PHIMS. • Ensures all users abide by the PHIMS Electronic Terms of Use Agreement. • Provides a yearly confirmation of all the Authorized Requestors for the site. • Ensures staff receive orientation and ongoing training about site/regional privacy policies and procedures. • Ensures all user(s) are PHIA compliant, and have signed a confidentiality pledge. • Ensures any privacy breaches or suspected breaches are investigated and PHIMS account termination is submitted when necessary.

Authorized Account Requestor	• Completes and submits the **Add/Modify/Terminate** account request form to the Shared Health Service Desk. • Compiles the users that require access to PHIMS in order to complete the tasks to perform their job. • Verifies that PHIA training has been completed. • Ensures Authorized Account Sponsor is aware of and approves all requests for PHIMS accounts and associated roles/permissions. • Ensures each user is provisioned with appropriate role(s) in PHIMS. • Ensures appropriate training has been provided to all new users (one-on-one or self-study), and users are aware of how to locate and access support material before and while using PHIMS. • Verifies if a new user already has an existing Shared Health network account. • Ensures user has completed an Authentication Questions and Answers form and that it has been submitted directly to the Shared Health Service Desk.

Privacy Reminders

Authorized Users may only access PHIMS for the following purposes:

- to provide health care, or for arranging for the provision of health care;
- for administrative responsibilities and duties related to supporting the provision of health care, or arranging for the provision of health care;
- to generate Standard Reports as prescribed in the Report User Guides (if applicable);
- to analyze surveillance data to inform timely public health action and response;
- to fulfill responsibilities and duties under The Public Health Act. PHIMS Authorized Users are required by law to keep confidential all of the information accessed in PHIMS and to comply with their employer's privacy and security policies.

PHIMS Authorized Users **must not:**

- access information out of curiosity or for personal use;
- look at their own electronic record;
- look at the electronic record of a friend, colleague, relative, family member or any other individual unless the Authorized User is in a professional care relationship with them.

Social Engineering/Phishing

Phishing is a type of social engineering (manipulation) where scammers attempt to steal confidential information such as usernames, passwords and financial information. Here is what you need to know to prevent this from happening to you.

- **Stay alert -** Suspicious email messages may be unexpected, urgent and/or try to instill fear.
- **Hover to discover -** Often, the scammer appears to be someone you know, but when you hover over the sender's name, email address or hyperlink, you may notice the sender is not really who they say they are. If you receive an email from someone you know but the email address is not one you recognize, follow-up with a phone call.
- **Click with caution -** If you receive any suspicious email messages that contain links or attachments, do not click on the links or open the attachments. Instead, report the email.

- **Report the message - Report suspicious emails to your local IT, or the Shared Health Service Desk.** Ensure to report any PHIMS-related phishing to the Shared Health Service Desk. The PHIMS Team may send direct links or attachments to users. We encourage you to always confirm the sender's identity as above if you are unsure about a message or link you have received. The PHIMS Team and the Shared Health Service Desk will never ask you to disclose your password.

Need support?
If you require support with PHIMS access or PHIMS software related issues, please contact the Shared Health Service Desk at:
Email: servicedesk@sharedhealthmb.ca (please state "PHIMS" in the subject line of the email)
Phone: (204) 940-8500
Toll free: 1-866-999-9698

For urgent matters contact the Shared Health Service Desk by phone and speak with an agent to escalate your request. Please consult with a peer supporter or trainer (if applicable for your organization) before logging any service requests.