SOMERSET WEST
COMMUNITY HEALTH CENTRE

IMPORTANT CYBER INCIDENT UPDATE: FACTS AND QUESTIONS

What happened?
Like many other organizations, we have been the victims of a cyber incident. This means that a third-party accessed our Information Technology (IT) systems without our authorization. The third-party encrypted (i.e., locked or otherwise blocked our access) some of our servers where we store our files.
As soon as we became aware of this, we shut down our wi-fi and network. We also immediately brought in cybersecurity experts to help secure our IT environment and to investigate what happened.

When did this incident occur?
We discovered this incident on April 30, 2026.

What have you done to address this incident?
Since discovering this incident, we have worked with cybersecurity experts to:

- Contain the incident and make our systems secure;
- Understand what happened and if any personal information was affected; and
- Improve our security and help prevent something like this from happening again.

We have also reported this matter to two government privacy offices: the Information and Privacy Commissioner of Ontario (IPC) and the Office of the Privacy Commissioner of Canada (OPC).

- The IPC oversees the protection of health information under the Personal Health Information Protection Act (i.e., for those who receive health services from us).
- The OPC oversees the protection of other personal information under the Personal Information Protection and Electronic Documents Act (i.e., for those who receive services from our community programs).

We have also told the police about this incident.

Is this affecting your services?
Our programs and services are now operational. We have communicated directly with clients if there are any exceptions.

Why didn't your IT security prevent the cyber incident?
We have worked closely with our IT service provider over the years to protect our IT systems. However, cyber threats are always evolving, and these kinds of incidents are not always preventable. Since this happened, we have worked with cybersecurity experts to improve our security and help prevent something like this from happening again. We are actively monitoring our systems to help protect against future threats. Keeping your information safe is very important to us.

Did you investigate the incident?
Yes, we brought in cybersecurity experts to help us investigate what happened. However, to keep our IT systems safe, we will not share any more details about the investigation.

Is the threat over?
Yes, the incident has been contained. We do not see any more signs of unauthorized activity.

Is it safe to provide personal information to SWCHC in the future?
An IT system cannot be 100% safe from every potential attack. That said, keeping your information safe is very important to us. We have worked with cybersecurity experts to improve our security and help prevent something like this from happening again. We believe the changes we made have made our systems safe, and we are continuing to closely monitor them to help protect your information.

Was my personal information compromised?
We do not know exactly what specific information may have been affected for each person. However, based on the investigation, we have identified the types of information that were accessed and/or taken by the unauthorized third-party. If you receive services from our Homelessness and Addiction, Recovery and Treatment (HART) Hub, Mental Health and Counselling, Ottawa Lung Health Program, Ottawa Newcomer Health Centre, or Primary Health Care, some or all of the following information about you may have been accessed and/or taken by the unauthorized third-party:

- Name
- Date of birth
- Home address
- Sex
- Phone number
- Driver's License
- Ontario Health Information Plan (OHIP) number
- Ontario Disability Support Program (ODSP) applicant number
- Client housing applications
- Name of healthcare provider
- List of medications
- List of allergies
- Medical, social and family history
- Symptoms
- Diagnosis
- Treatment plan
- Disability assessment
- Physical examination findings
- Test and imaging results
- Specialist referrals
- Specialist consult notes

According to our experts, there was no unauthorized access to our electronic medical records system, which contains the majority of our client personal health information.

Please visit www.swchc.on.ca/cyber-incident to read the full notice.

What can I do to protect myself?
We encourage you to be careful and watch out for common threats to your identity and personal information. Here are some steps you can take to protect yourself:

- Be careful when sharing your personal or health information, especially when the request is unexpected. If someone contacts you and asks you for your personal information out of the blue, do not share it.
- Do not click on links or download attachments in suspicious emails.
- If you receive a message that looks like it is from us asking for money or other personal information, and you were not expecting it, it may be a scam. Contact us directly to confirm before responding to the message.
- If you think that someone may be using your OHIP number without your permission, you can contact Ontario's Ministry of Health at 1-888-781-5556 Monday to Friday (excluding holidays), 8:30 a.m. to 5:00 p.m. or at reportohipfraud.moh@ontario.ca. They will look into it and may share your information with law enforcement if fraud is suspected.

Additional Questions.
If you have additional questions that are not addressed in the notice or FAQs, please reach out to our Privacy Officer at privacyofficer@swchc.on.ca.