ROSS MEMORIAL
HOSPITAL
Kawartha Lakes

December 21, 2023

Notice to Patients: Further Update Concerning February 2023 Cyber Incident

Dear RMH Community,

We wish to provide everyone with a further update regarding the cyber incident RMH experienced on February 5, 2023 (the “Incident”). As soon as the Incident was identified, RMH took immediate steps to contain and respond to the situation, and retained external third-party cybersecurity experts. This team conducted a detailed investigation and assisted RMH in restoring the security of our systems.

While the investigation has concluded, we are continuing to closely monitor the situation and have not detected any malicious use of data that may have been affected by the Incident.

Nevertheless, RMH has determined that a number of its systems – including its legacy MediPatient database – were so severely impacted by the Incident (through encryption and/or corruption), that some of its applications and data were rendered unusable. We wish to provide you with additional information given these findings.

What Happened?

- On February 5, RMH’s IT team was informed that staff were having difficulties accessing certain systems.
- The IT team immediately investigated these issues and identified unusual activity in the environment.
- As a result, RMH declared an IT Code Grey and retained external third-party experts to provide cyber incident response services to assist RMH in its containment, investigation, and recovery efforts.
- By February 6, 2023 (i.e., approximately 24 hours), the Incident was considered contained.
- Following our investigation, the personal health information (“PHI”) of 847 RMH patients was identified as having been affected and accessed without authorization. These patients have been directly notified by RMH.
- Other RMH databases storing legacy health information, including (for example) admission and discharge information, diagnostic imaging orders, and reports and consultation notes, were encrypted and/or corrupted because of the Incident, and several systems were left inoperable (e.g., MediPatient) (collectively, the “Corrupted Records”).
    - Corrupted Records include data in a file that *may* have been accessed without authorization, but it is impossible for RMH to confirm given the nature of the Incident and the state in which the data was left (i.e., it has become unusable, unreadable or inaccessible).

  - However, if data has been corrupted, RMH does not have any evidence to suggest this information was removed from our systems during the Incident.

How Might You Have Been Impacted?

The investigation identified that these Corrupted Records may have contained certain types of legacy patient data *if you were a patient at RMH between the 1960s and February 5, 2023.*

In such cases, a copy of your inpatient/outpatient visit information and/or physician dictation (e.g., Attending provider, Radiologist, Pathologist, Surgeon) was corrupted by the Incident. These Corrupted Records may have included the following types of PHI:

- OHIP number,
- Demographic information (name, address),
- Personal contacts (e.g., home address, next of kin],
- Lab results,
- Diagnostic Imaging results,
- Surgery results,
- Encounter details (e.g., visit date, providers, visit reason),
- Surgical encounter details (e.g., procedures, surgeon, attending providers, nurses, patient vitals, discharge status, vital status),
- PHS/HSM,
- Medication usage (e.g., ED and IP),
- ECG results,
- Falls and/or drug/med errors.

In most cases, RMH was successful in restoring records of visits and supporting documentation between the 1960s and Feb 5, 2023.

However, a subset of these Corrupted Records may have been impacted to the point where unfortunately, we are no longer able to access them.

Nevertheless, while this patient data may have been subject to unauthorized access, encryption, and/or corruption, there is no indication of any malicious use of PHI as a result of the Incident.

What Did We Do to Respond?

RMH took multiple steps to contain and remediate the Incident, including:

- Worked around the clock to remediate the Incident while also engaging leading third-party cybersecurity experts to conduct a detailed investigation into what happened.
- Immediately severing access to the Internet and all third-party networks, while maintaining our highest possible standards of patient care.

- Completing password resets for across the organization.
- Strengthening security controls and maintaining constant monitoring throughout the RMH environment.
- Notifying the Information and Privacy Commissioner of Ontario (“**IPC**”) in compliance with provincial health information legislation.

What Can You Do?

While there is no indication that any information involved in the Incident has been misused, we would like to remind you to be diligent in monitoring your accounts, and pay close attention for incidents of fraud and identity theft.

If you would like to get in touch with ServiceOntario regarding your health card number, you can visit any of ServiceOntario’s centres, their website, or call them (toll-free in Canada) at 1-800-267-8097.

As we noted above, the IPC has been notified of the Incident. To file a complaint, please visit: https://www.ipc.on.ca/resources/forms/

RMH will not contact you by email requesting you to provide or verify sensitive personal information. When in doubt or if you have any concerns about the validity of any emails RMH sends, please contact us as indicated below.

How Can I Get More Information?

If you have any questions regarding the Incident - or if you require further information or assistance - please call us at 705-324-6111, ext. 6284.

Should there be any further information about this Incident and your personal information, we will provide updates on this webpage.

Sincerely,

Kelly Isfan

President and Chief Executive Officer