NOVA SCOTIA
Health and Wellness
Office of the Minister

PO Box 488, Halifax, Nova Scotia, Canada B3J 2R8 • Telephone 902 424-3377 Fax 902 424-0559 • Health.Minister@novascotia.ca

August 30, 2018

Ms. Catherine Tully
Freedom of Information & Protection of Privacy Review Officer
Dept. of Justice
Suite 509, 5670 Spring Garden Rd.
Halifax, NS

Via Email: Catherine.Tully@novascotia.ca

Dear Ms. Tully:

I am writing in response to Investigative Report IR-18-01 on a breach within the Nova Scotia Drug Information System (DIS).

The Department of Health and Wellness appreciates the significance of this review and the valuable insights offered. We welcome the opportunity to strengthen privacy and confidentiality features in our information systems and note that digital health systems, like the provincial Drug Information System (DIS), provide an opportunity for better privacy monitoring and controls to protect personal health information.

Digital health systems are making significant contributions in improving patient care and informing patients about their health and care. Electronic digital management provides audit trail evidence that is time-stamped with a digital fingerprint to identify inappropriate access. This compares to paper-based systems (including fax machines) which are not effective in detecting when a privacy breach may have occurred, who had access to the information and what information they may have accessed. Digital health systems are not less secure than paper based systems. In fact, mechanisms to audit have improved and have been enhanced by the availability of digital audit and event logs. While citizens can be confident in these systems, it is important that the proper oversight is in place, that citizens are aware of their rights and that system users understand their obligations to protect personal health information or face consequences.

The Department believes in continual process improvement and works diligently to manage and protect personal health information. It is understood that even though digital health systems, such as the DIS; are not without potential privacy challenges, having an electronic system that controls data flow

between authorized or credentialed users eliminates many risks associated with paper forms. The enhanced ability to track access is one of the significant benefits of digital health systems like the DIS.

The ability to produce more than 60 privacy management documents for the Privacy Review Office when requested demonstrates the Department's commitment to protecting the privacy of citizens by ensuring policy and best practices are in place.

The following sections will itemize each recommendation and the Department's response.

Recommendation #1 – IR-18-01 - DIS Breach Investigation Protocol (Corrective Action Process)

I recommend that the DHW develop and implement an investigation protocol for the DIS. The protocol should:

i. Require that the Health Privacy Office of the DHW lead privacy breach investigations.
ii. Ensure that the Health Privacy Office has the authority to determine corrective action.
iii. Include a clear internal coordination protocol for any DIS privacy breach investigation.

Departmental Response

The Department will work with the pharmacy organizations to revise and strengthen the DIS protocol to ensure that information is forthcoming and complete when requested. The Department is developing an audit framework to document requirements needed to further support innovation and digital health systems. This will identify the requisite resources needed to support investigations.

Recommendation #2 – IR-18-01 - Containment

I recommend that the DHW re-contact all 46 affected individuals to determine if the pharmacist has been in contact with them since April 24, 2018. If so, I recommend that the DHW take further legal action to prohibit the pharmacist from further using or disclosing the personal health information she obtained as a result of these breaches.

Departmental Response

When a significant breach occurs, the Department complies with legislation, and reports the breach directly to the citizens impacted. For the DIS breach, the Department also took the additional step of providing courtesy notification to the Privacy Review Officer.

In March 2018, the Department issued a cease and desist letter to the pharmacist responsible for the breach. The letter was issued April 2018 and provided the following direction:

- Destroy all documents and other records (and any copies thereof, including hard copies and electronic copies) that contain personal health information obtained through the inappropriate access that is in your possession.
- Destroy all documents and other records (and any copies thereof) that contain personal health information obtained through the inappropriate access that you provided to others.

- Stop disclosing or using in any manner the inappropriately accessed personal health information, and the fact that you made such access.
- Provide the Department with a list of the individuals to whom you have disclosed personal health information obtained through the inappropriate access, and what personal health information was disclosed to each such individual.

The representative on behalf of the pharmacist involved responded to each of the directives and declared that there exists no continuing risk from the pharmacist to the individuals whose names and other information were contained in within the DIS. The response was received May 2018.

All impacted individuals were and are encouraged to contact the Department if they have further questions, concerns or complaints. A number of those that have contacted the Department requested and received the Request for User Access (RUA) and the Request for Personal Health Information (PHI) reports.

We will further notify all affected individuals and provide them with a link to the Investigative Report and Department Response and encourage them to contact the Department with any questions they may have.

Recommendation #3 – IR-18-01 - Electronic Database Breaches

I recommend that the Privacy Breach Protocol be revised to prescribe that where a user is found to have breached the privacy of any individual(s) via one of the electronic databases, detailed audits of that user's activity in other implicated databases be automatically conducted.

Departmental Response

This breach was the first of its kind and we take the recommendations for improvement seriously.

- The pharmacy system is integrated with the Client Registry and the DIS to better enable pharmaceutical care and service delivery for patients. Having access to an individual's medication profile when and where it is needed helps healthcare providers make better decisions about an individual's care. The Drug Information System increases the quality and safety of patient care for all Nova Scotians.
- The Department's Digital Health program incorporates privacy by design principles in all stages of the system life-cycle for digital health systems in the health environment.
- Digital health systems are subject to national, provincial and industry standards and assessments. The DIS was developed through extensive planning and implementation activities that include privacy and security input as well as essential input from the users and stakeholders who will access and benefit from these systems. The DIS completed Privacy Impact Assessments (PIAs) at each implementation stage as well as an overall Threat Risk Assessment (TRA).

The Department is committed to continual improvement and will review and revise the privacy breach protocol, as appropriate, based on the findings in the Investigative Report.

Recommendation #4 – IR-18-01 - Privacy Breach Notification

4(a) I recommend that the DHW immediately notify the two individuals who never received the first breach notification letter because the mail was returned unopened. I recommend that the DHW confirm with the OIPC when this step is completed.
4(b) I recommend that the privacy breach notification provisions in the DHW's Privacy Breach Protocol be revised as follows:

i. Clarify that notification at the first reasonable opportunity requires that notification occur within days (not weeks) of identification of affected individuals.
ii. Specify that notification need not await the identification of every affected individual and that notification can therefore occur as individuals are identified.
iii. Require that notification letters include, at a minimum, the following information:

- A clear and specific statement about what occurred and how it was discovered.
- A clear and specific statement about the personal health information that was accessed.
- Information about what the individual can do to mitigate potential harm.
- A clear and specific statement about steps taken to contain the breach and prevent it from happening in the future.

iv. Require that either the identity of the authorized individual who engaged in unauthorized access be provided in the notification letter or require that the record of user activity be enclosed with the notification letter.
v. Clearly advise affected individuals of their right to file a privacy complaint with the Office of the Information and Privacy Commissioner for Nova Scotia.

Departmental Response

On December 19, 2017, DHW notified the Privacy Review Office (PRO) of the breach and subsequent notification to the individuals affected, and arranged for a conference call with the PRO on December 20, 2017. During the conference call the notification letter was reviewed and the PRO provided feedback. The Department was notified of the formal Review Office breach investigation on December 21, 2017 and understood that the investigation was specific to the audit process. The investigation letter did not state any issue with the notification letters. The first batch of Department notification letters were issued on December 22, 2017. Final copies of the released letters were sent to the PRO on January 3, 2018.

For notification letters returned undeliverable, the Department will continue to assess our demographic resources for updated address information to attempt delivery. The Department will continue to review and revise notifications as required.

Recommendation #5 – IR-18-01 - Health Privacy 1-800 Line and Breach Investigations

I recommend that the DHW establish a protocol for investigating anonymous and other tips to its Health Privacy 1-800 line, beginning with communicating to all staff that anonymous tips can and should be followed-up.

Departmental Response

The Investigative Report (IR-18-01) noted that an anonymous caller had tipped the Department of potential inappropriate access in late May 2017, three months before the notification from the Nova Scotia College of Pharmacists.

The Department follows up on anonymous calls and will investigate, as appropriate. In this case, the Department's records indicate that a query was received with the caller providing their first name, phone number and indicating that a community pharmacy, which the caller did not identify, may be involved in a potential privacy issue. This call was followed up by the Department, however, no further information was forthcoming. Despite best efforts, there was no information provided in the anonymous tip on which an investigation could be initiated. It was not until the Department was notified by the regulatory college involved, that sufficient information was available on which to base an investigation.

Recommendation #6 – IR-18-01 - DIS User Agreement

I recommend that the DHW take the following actions with respect to the DIS User Agreement:
i. Enforce existing terms: The DHW should re-familiarize itself with its User Agreement and clarify internally the full extent of its authority and its responsibilities to manage and investigate a privacy breach by agents of a third-party user organizations under the Agreement.
ii. User organization audits: Require the DIS user organizations to regularly review access logs and conduct security audits of pharmacy software systems annually or more frequently.
iii. Monitoring of user organizations: Make the type and frequency of the DHW monitoring of user organization audits and audit capacity explicit and make the authority of the DHW to investigate privacy breaches involving the DIS explicit.
iv. Notification to DIS user organizations: Remind all DIS user organizations **by August 31, 2018** that they must comply with the DIS User Agreement requirement that they regularly review access logs and that, at a minimum, they must conduct security audits of pharmacy software systems annually.

Departmental Response

External access to the DIS medication profile is permitted through the Joint Service and Access Policy or JSAP. This policy obligates the user organization, or pharmacy, to advise DHW when they become aware of or reasonably suspect that a privacy or security breach has been raised. The policy also:

- defines the mutual responsibilities of the DIS Program and users of the DIS and ensures they are aware of the rules associated with accessing and providing access to the DIS;
- assists in the protection of privacy with respect to the personal health information collected, used, disclosed, and retained in the DIS;
- includes the Confirmation of Acceptance Form which must be signed by the User Organization before the DIS Program provides the User Organization with access to the DIS;
- provides direction on monitoring and auditing the DIS access connections and notes DHW's right to employ tools and applications as appropriate; and
- each user organization is provided with the DIS Privacy and Security Guidelines for Best Practices when the JSAP was executed.

The Department has an existing process in place to update the Joint Service and Access Policy (JSAP). The Department is reviewing the policy, specifically with respect to recommendation #6 and will update the policy and notify user organizations of their responsibilities accordingly.

Recommendation #7 – IR-18-01 - DIS User Training

I recommend that the DHW conduct training for all users of the DIS on the use of DIS notations.

Departmental Response

The Department believes that privacy and access training is essential to ensure citizen records are managed appropriately and to reinforce ethical principles. Higher standards exist for regulated health care professionals regarding protection of privacy and in many, if not all cases, licensing is directly impacted by abiding with obligations of privacy and access.

- Education for privacy and access is provided for two distinct groups: staff internal to the DHW and external support for partners and related entities such as agents[1] or stakeholders[2].
- DHW staff education includes both general privacy education provided by Internal Services Department (through the Information and Access group) and specific health privacy education delivered by our Departmental Health Privacy Office. For our external partners and related entities, Department training requirements are embedded in the external training materials.

The DIS is integrated with pharmacy practice management systems and functionality may vary among these systems; therefore, vendors and their associated help desks are responsible for end-user training. The Department works with the vendors and pharmacies to identify the appropriate level of training for all pharmacy users. The Department also contributes to continuing education through bulletins and on-line DIS training modules [3]and materials.

The Department will work with the vendors to ensure that DIS notation training is included in the pharmacy end-user training.

Recommendation #8 – IR-18-01 - The DHW Privacy Policy

I recommend that the DHW Privacy Policy be updated to reflect current position titles and to remove ambiguity about agency status of individuals not employed by the DHW.

Departmental Response:

The Department will update its privacy policy, as recommended.

---

[1] As defined in the Personal Health Information Act (PHIA) s3(a)
[2] Stakeholders include users from Regulated Colleges, Associations, Organizations, Bands
[3] As referenced at: https://novascotia.ca/dhw/ehealth/DIS/education-resources.asp

Recommendation #9 – IR-18-01 - DIS Audit Policy and Procedure

I recommend that the DHW develop more robust and systematic auditing policies and practices by taking the following steps:

i. The DHW either purchase its own version of the FairWarning platform for use on the DIS logs or arrange for direct access to the FairWarning platform held by the Nova Scotia Health Authority so that it can produce better and more effective audits.

ii. Update the audit criteria to include a requirement for proactive audits that flag:
- same name lookups,
- user organization employee lookups, and
- lookups without user notes and not associated with dispensing activity within one week before or two weeks after the look up.

iii. Within **six months** of this report, conduct audits to ensure that:
- All user organizations have the audit capacity to monitor access of staff to the DIS as required by the User Agreement. Where user organizations do not have such capacity, I recommend that the DHW ensure that an appropriate risk mitigation strategy is immediately implemented and that a FairWarning audit of all users within non-compliant user organizations is immediately conducted.
- All user organizations are maintaining a record of every security breach of the custodian's electronic information system as required by PHIA Regulation 10(3).

Departmental Response:

The Department acknowledges that there are opportunities for improvement by reviewing and revising our DIS Audit Policy and Procedure.

The Department has recently relocated the FairWarning audit report function for DIS from operational support at the Nova Scotia Health Authority (NSHA) to the audit team at the Department. Review and development of required audit activities and reports is underway.

Recommendation #10 – IR-18-01 - The DHW Privacy Policy Multi-User Electronic Health Records

I recommend that the DHW amend PHIA by adding provisions that assign responsibilities for interoperable health databases in use in Nova Scotia to prescribed entities as follows:

i. Assign specified duties to these prescribed entities including:
- manage and integrate personal health information received from custodians,
- ensure proper functions of the electronic health record,
- ensure accuracy and quality of personal health information,
- keep an audit log (record of user activity) with prescribed information requirements,
- keep an electronic record of all instances where a consent directive (s. 17 PHIA) is made, withdrawn or modified and include prescribed information requirements,
- audit and monitor records it is required to keep (consent directives, audit logs), and
- make available record of user activity, consent directives and audit logs at the commissioner's request.

ii. In developing and maintaining the electronic health record, require the prescribed

entities to:

- take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for developing and maintaining the electronic health record,
- prohibit employees from viewing, handling or otherwise dealing with personal health information unless the employee agrees to comply with the restrictions that apply to the prescribed organization,
- make available to the public and to each health information custodian that provides personal information to it a plain language description of the electronic health record and any directives, guidelines and policies of the prescribed organization that apply to the personal health information, and
- conduct threat and risk assessments including vulnerability and penetration testing with respect to the security and integrity of the personal health information.

iii. Set clear standards for privacy breach identification and notification to affected individuals, health custodians and the commissioner.

iv. Amend s. 5(1)(b) to make clear that prescribed entities are subject to PHIA and to the oversight of the OIPC.

Departmental Response

Current health privacy legislation supports the Department establishing an 'agent' type of relationship with other organizations, as appropriate. The Department will take the recommendation regarding prescribed entities under consideration.

In Closing

It is imperative that Nova Scotians and their personal health information are safeguarded in the systems we design. The Department will continue to design systems with privacy at the forefront of the development, including safeguards that promote innovation while protecting personal health information.

The Privacy Review Office investigative report identified several concerns with a "high-trust model". We appreciate insights gained through the investigation. The Department is reviewing this trust model with user organizations where components of our digital health systems are integrated with their in-house systems. The review will determine what changes are required.

I would like to thank both the Privacy Review Officer and departmental staff for their efforts before, during and after this breach and subsequent investigation.

Sincerely,

Randy Delorey, MLA
Minister