Office of the Information & Privacy Commissioner
Nova Scotia

OIPC

Investigation Report Update

Background

On August 1, 2018, the Office of the Information and Privacy Commissioner (OIPC) released two related investigation reports IR18-01 and IR18-02. The reports were the result of an investigation into a series of privacy breaches that occurred in relation to unauthorized access to personal health information in the Drug Information System (DIS). The investigation found that the Department of Health and Wellness (Department) does not have an adequate or effective breach investigation protocol, does not have effective administrative safeguards in place sufficient to protect Nova Scotians from "snooping" behavior, has failed to adequately audit the organizations who have been granted access to the Drug Information System and does not have sufficient safeguards in place to protect the database content of its broadly defined electronic health information systems.

With respect to the pharmacy, the OIPC's investigation identified that Sobeys failed to properly investigate the breach, did not adequately contain the breach and did not have an adequate technical capacity to detect unauthorized access to personal health information by authorized users.

The OIPC made 10 recommendations to the Department and 8 recommendations to Sobeys intended to mitigate the risks to Nova Scotians' personal health information. The reports both indicated that the OIPC would publish the responses of both organizations.

Department of Health and Wellness' Response

The Department of Health and Wellness submitted its formal response to the OIPC on August 31, 2018. The Department declined all OIPC offers to discuss the recommendations and implementation. The Department's full response is attached[1] and a summary of actions in response to each recommendation is set out below. The Department rejected the majority of the OIPC's recommendations. As a result, there are outstanding risks to the personal health information of Nova Scotians that have not been appropriately mitigated.

Sobeys' Response

Sobeys submitted its response to the OIPC on August 30, 2018 following engaged discussions and consultation with the OIPC. Sobeys has committed to taking meaningful action to fully implement the OIPC's recommendations. Sobeys' formal response is attached and a summary of actions in response to each recommendation is below. As a result of Sobeys' actions taken thus far and commitments to further action, the OIPC is satisfied that the identified risks are being appropriately mitigated.

[1] Note that the Department refers to the Information and Privacy Commissioner as "Review Officer" and "Privacy Review Officer" in its response. While the statutes continue to use those terms, in practice the title was changed three years ago to Information and Privacy Commissioner.

Investigation Report IR18-01 Update: OIPC Summary of the Department's Response

Recommendation	Summary of Response Provided	Response
#1: DIS Breach Investigation Protocol	• No action taken. • Fails to commit to clarifying the Health Privacy Office's authority and to taking the lead in DIS privacy breach investigations.	Not accepted
#2: Containment	• No action taken. • Fails to commit to asking affected individuals if the pharmacist was in contact with them.	Not accepted
#3: Electronic Database Breaches	• No action taken. • Contains factual errors. • Fails to commit to revising its privacy breach protocol to require that where a user is found to have breached privacy in one database that detailed audits of that user's activity in other databases be automatically conducted.	Not accepted
#4: Privacy Breach Notification	• No action taken. • Commits to assess "demographic resources" for updated address information to attempt delivery to individuals not yet notified of the breach. • Fails to commit to including specific notification requirements within its privacy breach protocol.	Not accepted
#5: Health Privacy 1-800 Line and Breach Investigations	• No action taken. • Contains factual errors. • Fails to commit to establishing a protocol for investigating anonymous tips and to communicating that protocol to staff.	Not accepted
#6: DIS User Agreement	• No action taken. • Commits to "review" the DIS User Agreement (the Joint Service and Access Policy) with respect this set of recommendations and "notify user organizations of their responsibilities accordingly." • Fails to commit to monitoring user organizations and to reminding user organizations of their audit requirements within the specified time period.	Partially accepted
#7: DIS User Training	• No action taken. • Commits to "work with the vendors to ensure that DIS notation training is included in the pharmacy end-user training."	Accepted
#8: The DHW Privacy Policy	• No action taken. • Commits to update its privacy policy as recommended.	Accepted
#9: DIS Audit Policy and Procedure	• "Relocated" the FairWarning audit report function for DIS to the Department audit team. • Begun review and development of "required audit activities and reports". • Fails to commit to conducting an audit of all user organizations to ensure that they have the audit capacity to monitor access of staff to the DIS and are complying with the DIS User Agreement.	Partially accepted
#10: Multi-User Electronic Health Records	• No action taken. • No commitment to take any action.	Not accepted

Investigation Report IR18-02 Update: OIPC Summary of Sobeys' Response

Recommendation	Summary of Response Provided	Response
#1: Breach Management Protocol	• Sobeys committed to revise its breach management protocol incorporating OIPC's guidance and provide training to staff responsible for privacy breach management. • Sobeys committed to taking these actions within six months.	Accepted
#2: Breach Notification	• Sobeys has notified 28 affected individuals that a false profile was created within its Pharmacy Management System. • Sobeys provided each affected individual with a paper copy of the profile.	Accepted & completed
#3: Delete False Local POS System Profiles	• Sobeys has permanently deleted the 28 false profiles from its Pharmacy Management System.	Accepted & completed
#4: Apply Provincial Health Privacy Law	• Sobeys has committed to immediately update its existing patient privacy brochures in Nova Scotia with sticker labels with the correct Nova Scotia information. • Sobeys has committed to printing new brochures for national distribution that directs individuals to a website with jurisdiction specific information. • Sobeys provided staff training to verbally communicate jurisdiction specific information to pharmacy customers.	Accepted
#5: Document Reasons for DIS Access	• Sobeys updated its Privacy Operations Standards to require pharmacists to document reasons for DIS access when there is no accompanying dispense activity. • In anticipation of this recommendation, Sobeys proactively required staff to acknowledge the updated documentation requirements in June/July 2018.	Accepted & completed
#6: Build Employee Confidence in the Workplace	• Sobeys committed to requiring all pharmacy staff to read the OIPC report and emphasize its corporate commitment to address issues that get reported. • Sobeys has begun in-person education with pharmacy managers. • Sobeys has committed to educating its staff about its Ethics Hotline and to post information about the Hotline in a prominent worksite location.	Accepted
#7: Strengthening the Continuous Quality Improvement Audit	• Sobeys increased its Continuous Quality Improvement Audit to occur twice per year, one to be conducted with non-management personnel. In addition, Sobeys has added privacy questions to its quarterly pharmacy manager checklist and has committed to introducing an annual privacy questionnaire performed by a district manager with both management and non-management staff.	Accepted
#8: Strengthening Technical Auditing	• Sobeys has implemented manual report audits of its Pharmacy Management System and portal access. • Sobeys has committed to identify and implement a technical audit solution either through its Pharmacy Management System or an add-on to that system.	Accepted