Summary of Department of Health and Wellness Implementation of Recommendations in IR18-01

Updated August 1, 2019

Recommendation #1: DIS Breach Investigation Protocol	
The DHW reviewed and clarified its internal processes and revised its Privacy Breach Protocol.	Complete
Recommendation #2: Containment	
The DHW contacted all the affected individuals it has been able to secure contact information for. It provided a link to the investigation report and highlighted the recommendations to the affected individuals.	Complete
Recommendation #3: Electronic Database Breaches	
The DHW revised its Privacy Breach Protocol to ensure that if a user is found to have breached privacy using one electronic database, an audit of that user's activity on all other department databases will be done.	Complete
Recommendation #4: Privacy Breach Notification	
The DHW revised its Privacy Breach Protocol to provide more clear timelines for notification to affected individuals and provided guidelines for the content of privacy breach notifications.	Complete
Recommendation #5: Health Privacy 1-800 Line and Investigations of Anonymous Tips	
The DHW clarified with staff that it can and will investigate anonymous tips it receives and provided a phone script to employees answering the Health Privacy 1-800 line.	Complete
Recommendation #6: DIS User Agreement & Monitoring of User Organization Compliance	
The DHW completed a baseline survey of existing pharmacy user organizations that demonstrates gaps in compliance with security auditing and user access monitoring. The DHW began the process to revise and update its user agreement, the Joint Service and Access Policy (JSAP for pharmacies). The DHW's most recent update on this recommendation indicates that the JSAP is in final draft and that it has yet to decide the type and frequency of monitoring it will do of user organization compliance with the JSAP. The DHW declined to provide the OIPC a copy of the draft JSAP. The privacy of citizen information contained in the DIS depends heavily on the user organization electronic security infrastructure and monitoring of user access. Implementation of this recommendation is critical to securing the personal health information in the DIS. To complete this recommendation, the DHW must: • implement a revised JSAP which makes compliance with information technology security and user access monitoring mandatory for user organizations; and • implement an effective monitoring of user organization compliance with mandatory information technology security and user access auditing and make the type and frequency of the compliance monitoring explicit to user organizations.	Incomplete
Recommendation #7: DIS User Training	
The DHW had pre-existing training delivered via on computer module which is consistent with this recommendation, but it does not track user completion of this training. It reported that it plans to track new user completion of the training once the JSAP user agreement is revised. The DHW has discussed training with the College of Pharmacists and asked pharmacy user organizations to refresh training with their existing users. No refresh of training with other users was reported. Users of the DIS include regulated pharmacists as well as a wide range of other regulated and unregulated agents of custodians. Current users work in pharmacies as well as medical clinics, physician offices and hospitals across the province. To underscore the DHW's leadership and control	Incomplete

over its database, it is important for users to hear directly from the DHW as the custodian of the Drug Information System. This recommendation was to conduct training with all users of the DIS. The DHW's activities to implement this recommendation fall short of full implementation because it has not conducted any training nor confirmed that training has been conducted and its activities focused only on pharmacy users and new users. To complete this recommendation the DHW must: • confirm that all existing users receive DHW training on the limits of their authority to access the personal health information in the DIS and on the use of notations to explain access that is not associated with dispensing activity.	
Recommendation #8: Update and Clarify the DHW Privacy Policy	
The DHW updated its Privacy Policy.	Complete
Recommendation #9: DIS Audit Policy and Procedure	
The DHW secured direct access to the FairWarning audit system to facilitate its audit practices. The DHW reported that it cannot implement the suggested audit flag for users looking up co-workers in the DIS and that it already uses the other flags suggested. The DHW did not report that its audit practices have been formalized or that it has implemented any changes to its audit criteria or processes. This recommendation was to develop more robust and systematic auditing policies and practices because the privacy breach activity investigated in this case went undetected by the DHW's auditing for over two years. The specific actions included in the recommendation suggested possible areas to improve the audits. During the investigation leading to IR18-01, the DHW's audit staff generated additional ideas for developing more robust and systematic auditing policies and practices, including increasing the sample size of random users audited at a time and excluding users recently audited when taking random samples of users to audit. My recommendation intentionally avoided these because the DHW is in the best position to determine the most effective measures to improve audit criteria, however, these suggestions would make the audit more robust and systematic. It is not clear why the DHW cannot implement the one specific criteria I did recommend (audit users who look up their co-workers), nor why it could not implement any other criteria to develop a more robust and systematic audit. The DHW reported that its risk mitigation strategy for non-compliant user organizations is: • its education/communications with the College of Pharmacists, student pharmacists, the Pharmacy Association of Nova Scotia, and user organizations; • its baseline survey of pharmacy user organization compliance with information technology security and user access monitoring; and • ongoing auditing of user access. None of these actions addresses the risks from non-compliant pharmacy user organizations. The DHW's activities to implement this recommendation fall short of full implementation. To complete this recommendation the DHW must: • formalize (document) more robust and systematic audit criteria and processes for monitoring user activity; and • implement a specific risk mitigation strategy for user organizations shown to be non-compliant on the DHW's survey.	Incomplete