Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada
Canada

Audit of the Management of Privacy Practices at Health Canada and the Public Health Agency of Canada

Final Report

November 2019

Table of Contents

List of Acronyms

ATIP	Access to Information and Privacy
HC	Health Canada
PIA	Privacy Impact Assessment
PIMSD	Planning, Integration and Management Services Directorate
PHAC	Public Health Agency of Canada
PMD	Privacy Management Division
PMF	Privacy Management Framework
PP	Privacy Protocol
SGBA+	Sex- and Gender-Based Analysis +
TB	Treasury Board

Executive summary

What we examined

We examined the management of privacy practices at Health Canada (HC) and the Public Health Agency of Canada (PHAC). All employees are responsible for privacy practices, but the Privacy Management Division (PMD), located within HC's Corporate Services Branch (CSB), leads the overall coordination of privacy efforts for HC and PHAC. PMD's responsibilities include the development of privacy policies, procedures, and practices; the delivery of privacy training and awareness programs to staff; assessing and reporting on privacy breaches; coordinating HC and PHAC input for InfoSource; and providing privacy analysis and advice using a number of tools, including Privacy Impact Assessments (PIAs) and Privacy Protocols.

This audit did not focus on how branches fulfill their responsibilities to assess and manage their own privacy risks in the delivery of their programs or services. We also excluded the management of Access to Information and Privacy (ATIP) requests.

Why are Privacy Practices important?

Both HC and PHAC possess and rely on the personal information of Canadians and protecting this information is vital. Privacy breaches could harm Canadians and damage the organizational reputation of HC and PHAC. This audit examined the effectiveness of personal information protection and provides Department and Agency management with recommendations on how to better protect personal information at HC and PHAC.

What was found

We found that key controls were generally in place and functioned as intended to effectively protect personal information.

We found that controls were sufficient in the following areas:

- HC and PHAC have a defined Privacy Management Framework (PMF) to outline its roles and responsibilities, and guide its work;
- There is an appropriate process in place for the management of privacy breach incidents; and
- Privacy Impact Assessments (PIAs) and Privacy Protocols (PPs) are prepared and approved by programs, and are reviewed by PMD.

We found that there were weaknesses in controls in the following areas:

- Without appropriate risk management, PMD was operating with limited organizational information and, as a result, its awareness efforts were mainly focused on the highest risk areas within its own branch, rather than being risk-based across HC and PHAC;
- While PIAs and PPs were prepared and approved to mitigate privacy risks, the recommendations made by PMD in the assessments were not being monitored by PMD; and
- Although some PMD staff had had training on Sex- and Gender-Based Analysis + (SGBA+), PMD had not documented an analysis of consideration of SGBA+ in its processes.

The audit makes four recommendations that will help to collectively strengthen the management of privacy practices for both HC and PHAC.

A. Introduction

1. Background

1. The *Privacy Act* governs the personal information handling practices of federal institutions. The *Act*, which came into effect on July 1, 1983, limits the collection, use, sharing, and disclosure of individuals' personal information. Under the *Privacy Act*, personal information is defined as information about an individual that is recorded in any form, and that can be used to identify an individual through its use, either alone or in combination with other information.
2. The Office of the Privacy Commissioner of Canada oversees compliance with the *Privacy Act* and aims to help federal institutions improve their personal information handling practices. The Privacy Management Division (PMD) and the Access to Information and Privacy (ATIP) Division manage the *Privacy Act* requirements for Health Canada (HC) and the Public Health Agency of Canada (PHAC). These shared services fall under the Planning, Integration and Management Services Directorate (PIMSD) of the Corporate Services Branch at HC.
3. Both HC and PHAC manage a large amount of Canadians' personal health information. While PMD and ATIP are primarily accountable for the administration of the *Privacy Act*, the protection of personal information is ultimately a shared responsibility between all employees at HC and PHAC.

B. Findings, Recommendations and Management Responses

1. Management Framework

4. We expected HC and PHAC to have a risk management approach for the protection of personal information. This would include a mechanism in place to identify and gather feedback directly from the branches on their privacy risks that would be used to create a privacy risk universe that would inform the Privacy Management Division's (PMD) efforts to target awareness activities across the two organizations.
5. PMD updated HC's and PHAC's Privacy Management Framework (PMF) in 2019 as part of its renewal efforts. The PMF identified the roles and responsibilities related to privacy for key stakeholders across the organizations and presents five key pillars for effective privacy management. Effective risk management was identified as one of the five key pillars in its PMF. However, this pillar was not further developed to establish how PMD would actually perform effective risk management, nor how PMD would build its privacy risk universe to inform effective departmental privacy risk management.
6. We found that PMD had developed guidance and tools1 to provide advice and assist branches in identifying their privacy risks for specific programs or initiatives, and reporting them back to PMD. PMD also provided recommendations on how to mitigate these specific privacy risks. PMD's review of these separate privacy assessments gave them an opportunity to gain knowledge of the various privacy risks across the organizations. We also found that PMD had numerous ad hoc conversations on privacy risks with the various programs who contact them for advice. This allowed PMD to gain a wealth of information on privacy risks. However, there was no collection or prioritization of these assessments and conversations into a privacy risk universe.
7. Overall, both HC and PHAC had a PMF identifying the need for effective risk management. However, they did not have a departmental risk management approach to assess and manage privacy risks at the departmental and branch level. Although no branch-level assessment was completed, PMD led risk-based activities identified in their draft strategic engagement plan. HC and PHAC would benefit from building a more strategic privacy risk universe to better inform PMD's operations, including targeted interventions and training and awareness campaigns.

Recommendation 1

The Assistant Deputy Minister, Corporate Services Branch, should strengthen branch risk management practices by conducting an Agency and Departmental risk assessment with input from all the branches.

Management response

Management agrees with the recommendation.

[1] For example: Privacy Impact Assessment Toolkit, the Privacy Handbook, the Privacy Occurrence report, the PMF and the Privacy Guidance when Contracting.

Management will continue to build on the targeted discussions that currently occur, as well as the privacy risk reporting that is done via the quarterly dashboards to HC and PHAC executive committees.

Planned actions recognize that program executives and senior officials who handle personal information are responsible for its compliant handling[1].

1. Directive on Privacy Practices. Section 6.2- 6.3

2. Privacy Impact Assessments and Privacy Protocols

8. Privacy Impact Assessments (PIAs) are used to identify the potential privacy risks of new or significantly modified programs or services that collect personal information for administrative purposes (i.e., when a decision is made about an individual). They also prescribe a plan to help eliminate or reduce those risks to an acceptable level. Privacy Protocols (PPs) are completed for programs or initiatives that have privacy implications for non-administrative personal information collection (i.e., personal information collected for research, audit, evaluation, statistical purposes, or as part of program delivery).
9. We expected that processes existed and were used effectively for the preparation of PIAs and PPs. We also expected that completed PIAs and PPs were approved and complied with the *Directive on Privacy Impact Assessments*.
10. We found that PIAs and PPs were prepared and approved to mitigate privacy risks. Appropriate processes were in place for the completion of PIAs and PPs, and were compliant with relevant policies and guidelines.
11. Since PIAs and PPs are initiated at the program level, there is the potential for gaps where programs may not be aware of their responsibilities or their required actions. PMD took the initiative to help identify privacy implications for programs or initiatives that may not have been aware of their responsibilities. This was mainly done by reviewing Memoranda to Cabinet (MCs) and Treasury Board Submissions for both organizations, as well as participating in the HC's Investment Planning processes.
12. We also expected that HC and PHAC monitored the implementation of recommendations made by PMD and privacy risk mitigation strategies developed by the program in the PIAs and the PPs.
13. We found that there was no process for following up on PIAs and PPs at the branch level. We could not find any evidence that either PMD or a third party monitored the implementation of the risk mitigation strategies outlined in the PIAs and PPs across all branches.
14. Overall, PIAs and PPs were prepared and approved to mitigate risks and comply with TB policies. However, there was no process in place for monitoring implementation of risk mitigation activities across all branches.

Recommendation 2

The Assistant Deputy Minister, Corporate Services Branch, should monitor and follow up on Privacy Impact Assessment and Privacy Protocol recommendations made by the Privacy Management Division.

Management response

Management agrees with the recommendation.

Planned actions recognize that program executives and senior officials who handle personal information are responsible for its compliant handling[2].

2. Directive on Privacy Practices. Section 6.2- 6.3

3. Breaches

15. A privacy breach involves improper collection, use, disclosure, retention, or disposal of personal information. A privacy breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders. The Treasury Board Secretariat (TBS) provides departments with Guidelines for Privacy Breaches, as well as a Privacy Breach Management Toolkit. Departmental privacy breach processes must adhere to the TB *Policy on Privacy Protection* and *Directive on Privacy Practices*.
16. We expected to find departmental policies or guidelines that describe how to identify, report, investigate, and remediate possible privacy breaches, and that such policies are in compliance with the relevant TB directives. We also expected processes to be in place for following up on breach reports and mitigation plans, and for monitoring trends in privacy breaches.
17. We found that PMD had created and distributed departmental guidelines, standard operating procedures, and checklists to assist programs, as well as guide its own internal operations on how to handle privacy breaches. Through document review, we found that these resources were aligned with the TB requirements.
18. We expected and found that completed privacy breach reports complied with TB and departmental policies.
19. Overall, procedures to identify, report, investigate, and remediate possible privacy breaches were well established.

4. Controls

20. While PMD is the centre of expertise for advice to programs and to support branches in complying with the Privacy Act, the protection of personal information is ultimately the responsibility of programs, as well as all HC and PHAC employees. Therefore, employee awareness is a key control for the protection of personal information.
21. We expected that HC and PHAC had a privacy awareness strategy that aimed at making the protection of personal information an integral part of the work culture and core values that guide all employees and managers at HC and PHAC. We also

expected that HC and PHAC had developed relevant privacy training materials that were accessible to all employees and managers, and that training and awareness campaigns existed to assist employees in remaining aware of their roles and responsibilities under the Privacy Act.

22. We found that awareness efforts in recent years had yielded limited engagement and rarely resulted in concrete outcomes. The efforts of recent years were described as insufficiently customized and directed to prioritize and address the specific needs of areas with high privacy risks. We found that PMD had recently tested its new training and awareness guidance and tools. However, these activities were mainly focused on the highest risks areas within its own branch, rather than being risk-based across HC and PHAC.

23. We found that PMD was engaged in promotional activities, such as communications via broadcast news and a kiosk during National Public Service Week. However, neither of PMD's privacy training courses was mandatory organization-wide. Privacy was once part of the new employees' onboarding training, but it was removed from the current mandatory onboarding training.

24. PMD conducted privacy training efforts at the National Microbiological Laboratory and, following an increase in awareness, the number of privacy questions directed at PMD increased. This underscores the importance of continuous awareness training.

25. We found that PMD was developing a strategic engagement plan that aims to use a risk-based approach to internal communications, with the objective of improving those privacy awareness and practices at HC and PHAC that are perceived as being of highest risk.

26. Overall, we found gaps in awareness efforts. PMD has been operating with a draft engagement plan and its efforts were mainly focused on the highest risk areas within its own branch. HC and PHAC would benefit from increasing their awareness efforts in a risk-based manner across the two organizations.

Recommendation 3

The Assistant Deputy Minister, Corporate Services Branch, should finalize and implement the Privacy Management Division's strategic engagement plan, in order to fully implement its training and awareness strategy across the two organizations in a risk-based and strategic fashion.

Management response

Management agrees with the recommendation.

The strategic engagement plan has been used since December 2019 to identify areas of highest risk and has subsequently allowed for PMD to prioritize its engagement work at the Departmental and Agency level.

Branches within HC/Agency manage various amounts and types of personal information depending on their mandates, therefore the actions outlined will be prioritized in consideration of branch-specific risk assessments.

5. Sex- and Gender-Based Analysis+

27. We expected PMD's staff to have completed the Sex- and Gender-Based Analysis + (SGBA+) training and that SGBA+ had been incorporated into PMD's business processes where appropriate2.

28. We found that three out of 18 PMD staff members had completed SGBA+ training. One of these three was found to have extensive knowledge of SGBA+. We found that PMD had conducted an analysis on how SGBA+ could be incorporated into PMD business processes.

29. In conclusion, although some PMD staff members have had SGBA+ training, PMD had not documented an analysis of consideration of SGBA+ in its processes.

Recommendation 4

The Assistant Deputy Minister, Corporate Services Branch, should ensure that all Privacy Management Division staff have completed basic Sex- and Gender-Based Analysis + training and assess where SGBA+ may be relevant to its business practices and tools.

Management response

Management agrees with the recommendation.

[2] We did not consider SGBA+ outside of PMD and how SGBA+ considerations are taken into account when dealing with personal information by programs. However, this consideration is part of the performance of OAE's audits when auditing a specific program.

C. Conclusion

30. The objective of this audit was to determine whether personal information at HC and PHAC was effectively protected.

31. We found that key controls were generally in place and functioned as intended to effectively protect personal information.

32. We found that controls were sufficient in the following areas:

- HC and PHAC have a defined Privacy Management Framework (PMF) to outline its roles and responsibilities and guide its work;
- There is an appropriate process in place for the management of privacy breach incidents; and
- Privacy Impact Assessments (PIAs) and Privacy Protocols (PPs) are prepared and approved by programs and are reviewed by PMD, as per the Treasury Board (TB) *Policy on Privacy Protection*.

33. We found that there were weaknesses in controls in the following areas:

- HC and PHAC do not have a documented risk management framework for privacy across their organizations. Without appropriate risk management, PMD was operating with limited organizational information and, as a result, its awareness efforts were mainly focused on its own branch, rather than being risk-based;
- While PIAs and PPs were prepared and approved to mitigate privacy risks, the recommendations made by PMD in the assessments were not being monitored systematically; and
- Although some PMD staff had taken SGBA+ training, PMD had not documented an analysis of consideration of SGBA+ in its processes.

34. The audit makes four recommendations that will help to collectively strengthen the management of privacy practices for both HC and PHAC.

Appendix A – Lines of Enquiry and Criteria

Audit of the Management of Privacy Practices at HC and PHAC
Audit Criteria
1. HC and PHAC have a risk management framework to assess and manage privacy risks at the departmental level.
2. Privacy Impact Assessments (PIAs) and privacy protocols are prepared, approved, and monitored to mitigate risks.
3. Procedures to identify, report, investigate, and remediate possible privacy breaches are established and operating as intended.
4. Controls exist for the protection of personal information.
5. SGBA+ considerations are taken into account when dealing with personal information

Appendix B – About the Audit

1. Audit Objective

The audit objective is to determine whether personal information at HC and PHAC is effectively protected.

2. Audit Scope

The scope of this audit included key departmental structures, processes, and practices pertaining to the management of privacy practices at both HC and PHAC.

The audit excluded the management of ATIP requests. The audit excluded the physical security and safeguard of personal information (encryption of data and locked cabinets), as well as the Information Management (IM) lifecycle, since these were assessed during recent audits of physical security and information management.

3. Audit Approach

The audit was conducted in accordance with the Government of Canada's *Policy on Internal Audit* by examining and gathering sufficient and relevant evidence to provide a reasonable level of assurance in support of the audit conclusion.

The audit examined the design and operation of HC and PHAC's privacy management practices, as measured against the requirements of the *Privacy Act* and its supporting policies and directives.

The Audit approach included, but was not limited to:

- A review of relevant documentation, policies, standards, guidelines, and frameworks;
- Observations and interviews with key officials at PIMSD and branches programs with responsibilities related to the handling of personal information;
- Testing of privacy management practices (detailed testing of related controls over privacy management practices) from sampled PIAs, privacy information banks, Privacy Protocols, Information-Sharing Agreements, and contracts; and
- Analysis of findings from interviews, inquiries, document reviews, and detailed testing.

4. Statement of Conformance

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing,* and is supported by the results of the Office of Audit and Evaluation's Quality Assurance and Improvement Program.