Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Privacy Audit of the Treasury Board Secretariat Claims Office

Published: 2024-09-09

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT53-38/2024E-PDF
ISBN: 978-0-660-73519-1

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Audit de la protection des renseignements personnels du Secrétariat du Conseil du Trésor du Canada Bureau des réclamations

Privacy Audit of the Treasury Board Secretariat Claims Office

On this page

Message to executives

▶ In this section

The Treasury Board of Canada Secretariat's Claims Office has established and maintained an adequate privacy management framework to safeguard the privacy of claimants' information, including the identification and mitigation of privacy risks.

Opportunities to enhance privacy management practices were identified in order to strengthen the protection of claimants' data. These opportunities include:

- offering complete information on how the personal information bank (PIB) collects medical data for claimants
- developing action plans

- improving the mechanisms for tracking all privacy impact assessment (PIA) risks and recommendations

Additionally, once the ongoing litigations are complete, the Claims Office should implement its disposal plan, with clear timelines and protocols.

Significance

The Claims Office handles a large volume of claimant personal information to resolve claims, making it crucial to ensure that this information is well protected.

Objective

Provide assurance on the adequacy of the Claims Office's privacy management practices, including actions taken to mitigate risks identified in PIAs.

Scope

The audit focused on the Claims Office's management of claimant personal information, privacy practices, IT controls and actions mitigating medium to high risks identified in other privacy-related assessments.

The audit excluded the assessment of claims processing, the validity of decisions and the use of funds in claims settlement.

Results at a glance

▶ In this section

Observations

1. The PIB description does not include the Claims Office's collection of medical information.

2. The Claims Office has retained all claimants' data since its inception because of ongoing litigation and the complexities of differing retention periods. Upon conclusion of these litigations, the Claims Office plans to implement data disposal strategies.
3. There was no monitoring to demonstrate how the Claims Office's PIA recommendations and concerns were considered, addressed and implemented. For example, four recommendations, two of which were high risk, were not implemented and did not have a documented rationale for not being implemented.

Management considerations

1. To ensure transparency, the Claims Office should consider updating the online description of the Claims Office Program's holdings to ensure that it is accurate and complete, including a clear reference to the collection of medical information.
2. To ensure the protection and privacy of information, upon resolution of all litigation and legal processes, the Claims Office should consider reviewing and potentially revising its disposal plan for claimant personal information. This plan should include specific timelines and protocols that comply with the varying retention periods.
3. The Claims Office has considered and integrated past PIA recommendations. To ensure a transparent decision process, the Claims Office should consider documenting the rationale for any recommendations not implemented.

Context

The Claims Office was established by the Government of Canada to provide guidance and a consistent approach to resolving claims of former and current employees who had incurred out-of-pocket expenses, had government benefits disrupted, or had impacts on income taxes and government benefits, as well as claims for severe personal or financial

hardship incurred as a result of the Phoenix Pay system. The Claims Office operates the Government of Canada–wide claims process in accordance with the various Phoenix pay system damages agreements negotiated between the Treasury Board of Canada Secretariat as the employer and all core public administration bargaining agents. The Claims Office assesses claims and recommends resolutions that are to be implemented or paid by the claimant's home department.

Significance of this audit

To resolve claims, the Claims Office handles a large volume of claimant sensitive personal information. This process involves interactions with multiple departments and agencies, making it essential to ensure the protection of claimant personal information. This audit was initiated to fulfill a recommendation from the Office of the Privacy Commissioner of Canada (OPC) about the PIAs conducted by the Claims Office.

Audit overview

See Appendix A for more details on the scope and methodology of the audit. See Appendix B for more details on the lines of enquiry and accompanying audit criteria.

Scope

1. The audit focused on the Claims Office's claimant personal information management, privacy practices, IT controls and actions mitigating medium to high risks identified in prior privacy-related assessments.
2. The audit excluded the assessment of claims processing, the validity of decisions and the use of funds in claims settlement.

Methodology

This audit conforms with the International Standards for the Professional Practice of Internal Auditing and included the review and analysis of documents and interviews and the testing of controls.

Results

1. Privacy practices: governance

The Treasury Board's *Policy on Privacy Protection* provides direction to government institutions to ensure compliance with the *Privacy Act*. The Claims Office is expected to apply the policy by providing clear guidance on roles and responsibilities, outlining standard practices for managing personal information, and ensuring proper training that aligns with privacy expectations.

Observations

The Claims Office has demonstrated its commitment to protecting personal and sensitive information through the effective implementation of privacy management practices. Some notable examples include:

- The Claims Office has established standard operating procedures for claims processing, outlining the roles and responsibilities of both claimants and staff.
- The Claims Office relies on PIAs to guide its employees in the daily management and handling of privacy issues.
- An information-sharing agreement is in place with Public Services and Procurement Canada to support compliance with the *Privacy Act* in protecting pay-related information.
- While collecting data, the Claims Office implemented data checks to mitigate the risk of errors in claim submission.
- Access controls for the client relationship management (CRM) system have been implemented to reinforce privacy protection.

- The Claims Office mandates that all new employees undergo privacy and security training and that all staff complete an annual refresher course as part of their performance management agreement.

Impact

An effective governance framework, complete with clear guidance on roles and responsibilities and comprehensive training, mitigates privacy risks and helps maintain public trust.

2. Privacy practices: data collection, storage and disposal

Under the *Policy on Privacy Protection* and the *Directive on Privacy Practices*, it is expected that:

- personal information is collected legally, stored securely and disposed of responsibly
- the collection of personal information is necessary and limited
- individuals are informed of their rights
- access is restricted
- disposal methods are secure, reflecting a commitment to privacy throughout the information's life cycle

Observations

- The PIB describes the personal information held by a government department, ensuring transparency, privacy and accountability in how data related to human resources, travel and administrative services is handled.
- The description about the information being collected and retained for compensation for damages (for example, TBS PCE 742 in the PIB) did not identify medical records. Given the sensitivity, claimants should be aware of how this information is collected, used and retained.
- Since its establishment, the Claims Office has not disposed of any data due to ongoing litigation and the complexities of varying retention periods. Considering ongoing litigation requirements, it may be

necessary to review and possibly revise the Claims Office's plans for the retention and disposal of claimant data.

Impact

The omission of claimant medical information from the PIB description could increase transparency issues and the risk of non-compliance with relevant policies and directives.

3. Privacy risk assessment

The *Policy on Privacy Protection* expects heads of institutions to establish practices for the protection and management of personal information, including conducting compliance reviews and adhering to the *Privacy Act*. The OPC and the *Directive on Privacy Impact Assessment* require departments to conduct PIAs in compliance with the *Privacy Act* as part of the effective management of privacy risks.

Observations

- The Claims Office conducted an initial PIA in 2017. Following significant changes to the Phoenix damage claims program, two additional PIAs were completed in 2019 and 2021. The culmination of these efforts is reflected in the consolidated PIA dated September 2022.
- In accordance with the *Directive on Privacy Impact Assessment*, organizations are required to submit their completed PIA reports to the OPC. The consolidated PIA was submitted on March 4, 2024, to the OPC for review.
- Most of the 46 PIA recommendations have been addressed:
    - 27 have been fully implemented
    - 10 are in progress or partially implemented
    - 5 have not been implemented and management has accepted the risk with justification (1 is high risk, 2 are medium risk and 2 are low risk)

    - 4 have not been implemented without documented justification (2 are high risk, 1 is medium risk and 1 is low risk)
- Action plans were embedded into the PIA of 2019. There were no action plans in the PIA of 2017, PIA of 2021 and the consolidated PIA of September 2022. There were no records or evidence of monitoring to demonstrate how PIA recommendations, risks and concerns were considered, addressed and implemented.

Impact

The absence of documented action plans and the incomplete implementation of PIA recommendations currently weaken the effectiveness of privacy management practices in the claims process. Establishing a system to monitor privacy risks and recommendations from PIAs and other assessments would strengthen the timely implementation of mitigation strategies and enhance the overall management and oversight of privacy issues.

See Appendix C for details on areas for management consideration and accompanying management responses.

Appendix A: About the audit

▶ In this section

Authority

The Advisory Claims Office – Privacy of Information was identified on the Treasury Board of Canada Secretariat 2022–23 Integrated Audit and Evaluation Plan.

Statement of conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing (ISPPIA).

Objective and scope

The audit objective was to provide assurance on the adequacy of the Claims Office's privacy management practices, including the actions taken to mitigate risks identified in PIAs.

The scope of this audit included the Claims Office's management of claimant personal information, including its privacy practices and its supporting processes, tools and IT-enabled controls.

The scope also included a review of privacy-related assessments (such as PIA, Threat Risk Assessment, Security Assessment and Authorization), and greater focus was given to assessing the mitigation of risks and concerns rated as medium or high.

Scope exclusion

The audit excluded the efficiency and effectiveness of claims processing and the validity of claims decisions, as well as the expenditure of funds to settle claims.

Methodology

The audit approach and methodology conformed with the ISPPIA. Methodology for this audit included but was not limited to:

- review and analysis of documentation, including analysis of privacy-related assessments
- interviews and written responses to questions with key partners, such as Claims Office staff, the departmental Access to Information and Privacy Office, and TBS's Information Management and Technology Directorate staff responsible for system security, infrastructure and operations related to privacy practices
- review and testing of system controls for ensuring claimant privacy (such as the CRM system and the claims portal)

In line with the scope exclusion outlined above, and to ensure that privacy of claimants was maintained:

- processing of individual claims was not tested
- an onsite walk-through inspection of the Claims Office was not carried out
- personal information of claimants was not requested, viewed or collected

Appendix B: Lines of Enquiry and Accompanying Audit Criteria

The audit covered the following line of enquiry.

Line of Enquiry 1: The Claims Office conducts operations with due regard for privacy of claimants' information, including the identification and mitigation of privacy risks.

Audit criterion 1.1

There is an effective management control framework in place to ensure that the personal information of claimants is adequately managed, including its collection, storage, safeguarding, access and disposal.

Audit criterion 1.2

Privacy risks identified in PIAs or through other means are efficiently managed and mitigated.

Appendix C: Management Response

▶ In this section

To enhance the protection and privacy management of the claimants' data, several key considerations were identified. Management is asked to identify a response and action plan to address these key considerations.

Given that the observations were presented for management's consideration, the management response and action plan will not be included as part of the Internal Audit and Evaluation Bureau follow-up process.

Management consideration 1: data collection, storage and disposal

To ensure transparency, the Claims Office should consider updating the online description of the Claims Office Program's holdings to ensure that it is accurate and complete, including a clear reference to the collection of medical information.

Management response:

Agreed.

Management action plan:

In collaboration with SCMA-ATIP and TBS Legal Services, the Claims Office will update the online description of the program's holdings to include clear reference to the collection of medical information for severe impact claims.

Due date:

December 31, 2024

Responsible:

Office of primary interest:

- Claims Office

Other stakeholders:

- SCMA-ATIP
- TBS Legal Services

- OCHRO-ERTC
- bargaining agents, if required

Management consideration 2: data collection, storage and disposal

To ensure the protection and privacy of information, upon resolution of all litigation and legal processes, the Claims Office should consider reviewing and potentially revising its disposal plan for claimant personal information. This plan should include specific timelines and protocols that comply with the varying retention periods.

Management response:

Agreed. The Claims Office operates under multiple legal authorities, each with specific retention and disposition requirements. Claims retention is further complicated by the Memoranda of Agreement on Phoenix Damages. Information must also comply with multiple government-wide litigation hold requirements. The Claims Office has an information retention and disposal plan based on the types of information collected and used in the claims process.

Management action plan:

Once litigation is complete, on a case-by-case basis, the Claims Office will review the current retention and disposition protocol (and update accordingly as required) and will implement the retention periods and disposal of claimant personal information.

Due date:

Within 90 days of official notification of litigation process completed.

Responsible:

Office of primary interest:

- Claims Office

Other stakeholders:

- SCMA-ATIP
- OPC for consultation

Management consideration 3: privacy risk management

The Claims Office has considered and integrated past PIA recommendations. To ensure a transparent decision process, the Claims Office should consider documenting rationale for any recommendations not implemented.

Management response:

Agreed. As part of the PIA updates in 2017, 2019, 2021 and 2022, the Claims Office reviewed and evaluated the recommendations of the previous PIAs. The Claims Office consolidated this information and updated the subsequent PIA based on current circumstances, reviewing and identifying any new and emerging risks and subsequently developing and implementing risk mitigation strategies within the new PIA document itself.

Management action plan:

The Claims Office has reviewed and updated the consolidated 2022 PIA and submitted it to the OPC for consultation and review (March 2024). The Claims Office will incorporate any comments received from the OPC. The Claims Office will also document rationales for any recommendations not implemented.

Due date:

December 31, 2024

Responsible:

Offices of primary interest:

- Claims Office

- SCMA-ATIP

Other stakeholders:

- OPC for consultation

[ISBN: 978-0-660-73519-1]

Date modified:
2024-09-12