Protecting Personal Information When Teleworking

Context

This guidance is intended to support public servants in their responsibility to protect personal information and prevent privacy breaches when teleworking.

Teleworking has become the new norm for many public servants. While this offers new opportunities to explore more digital ways, the introduction of teleworking has changed the way public servants create and manage information and collaborate with others. These changes have resulted in new challenges to established workplace processes, information management practices, service delivery and internal collaboration that are protected within the security of Government of Canada facilities and network environments.

When teleworking, the *Privacy Act* and its related TBS policy suite outline the requirements that federal institutions and their employees must fulfill in order to protect the personal information under their control. Additionally, under the *Policy on Service and Digital*, privacy must be addressed in the context of any plan or strategy to manage departmental information or data.

The information provided below offers some tips and helpful resources to protect personal information and prevent privacy breaches when teleworking.

Privacy Breaches

A privacy breach is the improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information.

What to do if you suspect a privacy breach has occurred:

You must report any suspected privacy breach to your institution's Access to Information and Privacy Office (ATIP) office and follow your institution's plans and procedures for privacy breach management. The Privacy Breach Management Toolkit provides guidance on how to support the management of privacy breaches. In addition, your institution's ATIP office will be able to provide you with more specific information and the next steps.
The table below outlines scenarios and considerations to guide you in preventing and managing potential privacy breaches when teleworking.

Related References:

- Policy on Privacy Protection
- Policy on Government Security
- Directive on Privacy Practices
- Directive on Service and Digital
- Privacy Breach Management Toolkit

Other content specific links are found directly in the text below.

Scenario 1: In telework situations, employees may use digital collaboration or productivity tools to connect with others or advance their work.

What to consider?

It is important to note that some personal information about public servants such as your name, title, classification, work email address and work phone number is not considered to be protected personal information by the Privacy Act.

Q: Do I have to provide personal information such as my personal phone number or personal email address in order to use digital collaboration tools in the workplace?
A: No. Productivity or collaboration tools used in carrying out your duties and functions as a public servant should only require work-related contact information.

Q: When using collaboration tools or virtual meeting tools, I may need to discuss sensitive personal information about an identifiable individual. Is that appropriate?
A: It is often necessary to discuss sensitive personal information in the course of your duties and functions as a public servant. For example, Labour Relations employees discuss sensitive personal information with managers. When using digital tools to communicate personal information, before using a new tool, contact your information management, security and privacy officials to ensure that the specific tool is appropriate in your situation.

Q: I am invited to use a virtual meeting tool that uses video images. I am not comfortable sharing my video image. Does the Privacy Act have any requirements that I should be aware of?
A: An image is personal information when it is about an identifiable individual and recorded in any form. Therefore, if your image is being recorded through the tool it must be protected in accordance with the *Privacy Act* and related policy instruments.

If you are not comfortable using the video features of a virtual meeting tool you should first discuss your concerns with your manager. They will be able to provide you with more assistance on the best way forward. Often, virtual meeting tools have features that allow for participation without using the video feature.

Q: I have installed home assistants (Google, Alexa, etc.) throughout my house, can I still telework?
A: Yes, but you should always take precautions against inappropriate disclosures of personal information when teleworking. This includes removing or turning off the passive listening device from your workspace. The *Privacy Act* and government security and privacy policies require the protection of personal information and passive listening devices could pose an additional privacy risks, such as inadvertently collecting and disclosing information. Please contact your institution's ATIP office and Chief Security Officer for further information.

Scenario 2: In telework situations, employees may bring hard copy documents containing personal information about an identifiable individual into their home environment.

What to consider?

To prevent privacy breaches from occurring in your telework environment you should have a dedicated area where you can reduce the entry of incidental visitors (E.g.: family members, guests, workers). As per the Directive on Service and Digital, ***digital systems are the preferred means*** *of creating, capturing and managing all information. Working remotely on hard copy documents containing personal information should be avoided whenever possible. In instances where this is not possible, documents containing personal information should be stored appropriately and, when no longer needed, destroyed appropriately. Please refer to the Directive on Security Management - Appendix J: Standard on Security Categorization, and/or contact your institution's information management and security offices for further detail.*

Q: What is the security designation of personal information?

A: That depends on the nature of the personal information. For instance, contact information about an identifiable individual is typically designated as Protected A, while medical or tax information about the same individual is typically considered Protected B. Protected C personal information should only be processed on a system accredited to that security designation and, as a rule, within a designated Government of Canada (GC) worksite. GC employees are prohibited from working on Protected C information from home without obtaining written permission from the approved authority. CSOs or higher-level management up to the Deputy Head are responsible to risk manage authorizations for employees to process and store all categorizations of hardcopy information at the telework location.

Regardless of the security designation of the personal information, any inappropriate creation, collection, use, disclosure, retention or disposition of the personal information is a privacy breach.

Q: How do I know the proper techniques for securing and transporting hard copy records containing personal information?

A: Information specific to the secure storage, transport, transmittal and destruction of documents when teleworking is best obtained from your manager or alternatively, your institution's security and information management offices. It will be important that the carrying case, lock, mode of transportation and the at-home storage be appropriate for the security designation of the information. The following link also has further guidance on managing information while teleworking.

Scenario 3: In telework situations, employees may need to deliver services in a new way, while continuing to protect personal information.

What to consider?

To protect against privacy breaches while delivering services when teleworking, you should consider how the change to the delivery model affects the management and flow (creation, collection, use, disclosure, retention, disposal) of personal information, and work with your ATIP office to determine if these changes require a Privacy Impact Assessment or a privacy protocol. Please refer to the requirements in the Directive on Privacy Practices or contact your institution's ATIP office for further details.

Q: How does changing service delivery from an in-person model to a hybrid telework model affect the management of personal information?
A: That depends on the institution as well as the program or service and tools employed in the process. For instance, some services may use new technology or third-party providers to deliver information to the service recipient. This could result in a new, and possibly unauthorized creation, use, disclosure, retention or disposal of personal information thereby resulting in a privacy breach. For example, if a third party contracted by the GC retained a copy of personal information for its own commercial purposes while delivering a service on behalf of the GC, this would be considered privacy breach. Alternatively, a new tool or technology could require the collection of additional personal information that is not directly related to the program or activity employing the new tool or technology. This new collection could constitute a privacy breach. To assess changes to business processes and their impact on the management of personal information, service delivery programs should work with their IM and ATIP offices to determine whether a Privacy Impact Assessment or privacy protocol is required.

Q: How do I know if changes to a business process are aligned with privacy requirements?
A: The privacy requirements that GC institutions are required to fulfill are found in the *Privacy Act* and its related TBS policy suite as well as in institution-specific legislation and policies. Please work with your IM and ATIP offices to discuss any changes to business processes that may affect the management of personal information to ensure that personal information will continue to be protected.

Scenario 4: In telework situations, employees need to ensure that they are saving records to the appropriate corporate repositories.

What to consider?

The inappropriate retention or disposal of personal information can lead to privacy breaches. To prevent this from occurring in a telework environment, employees should save records of business value to designated corporate repositories. This includes classifying records according to an institution's corporate file plan, attributing the appropriate security designation to each record and ensuring that the repository is accredited to store, at a minimum, the same designation as the document. Please refer to the Directive on Service and Digital or contact your institution's IM and security offices for further details.

Q: Can I save records containing personal information locally on my work computer when teleworking?
A: No. Your work computer is not an official corporate repository. There may be times when it is necessary to do so, but this should only happen when necessary and for a limited period. For example, should you lose network connectivity and need to save the record, saving the record locally is permitted provided that when you connect to the network again, the record is saved in the appropriate repository.