BRITISH COLUMBIA | Ministry of Citizens' Services

Guidance on Ministerial Order M431

Respecting Disclosures During the COVID-19 Pandemic

Summary

- On March 26, 2020 the Province issued Ministerial Order 085. Ministerial Order 180 was signed on June 3, 2020 and extended the disclosures authorized by Ministerial Order 085 until December 31, 2020. Ministerial Order M431 was signed on November 30, 2020 and extends the disclosures authorized by Ministerial Order 180 until May 31, 2021. This order authorizes public bodies to disclose personal information outside Canada in a way that, under normal circumstances, would not be supported by the *Freedom of Information and Protection of Privacy Act* (FOIPPA).
- This order is intended to remove a barrier that currently prevents employees in the B.C. public sector from using certain third-party applications and tools (e.g. for video conferencing or messaging) for communication and collaboration.
- Before any new third-party applications and tools can be used, certain conditions must be met (see page 3).
- This order has been issued in the public interest. During the COVID-19 public health emergency, the use of such tools by the B.C. public sector may be essential for maintaining operations and supporting directives of the Provincial Health Officer.
- The disclosure authority is temporary. It took effect on March 26, 2020 and expires on May 31, 2021 unless otherwise rescinded or extended by the Minister of Citizens' Services.

Authority to make this order

Ministerial Order M431 was created under section 33.1(3) of FOIPPA to allow the disclosure of personal information outside Canada in specific circumstances:

- Health care bodies, the Ministry of Health, the Ministry of Mental Health and Addictions, and the Provincial Health Services Authority may disclose personal information outside Canada for specific purposes related to the COVID-19 pandemic.
- Additionally, public bodies, including ministries, may use available technologies, defined as third-party applications and tools, which may be hosted outside Canada, to support and maintain the operation of programs or activities and communication during this time of rapid change and public health emergency.
- It is important to note the conditions for the use of these tools, including that they are reasonably secure, that personal information is removed from the tools as soon as

possible when this time period is concluded and that records created using these tools are managed appropriately.

About the Ministerial Order

Under Ministerial Order M431:

1. Health care bodies, the Ministry of Health, the Ministry of Mental Health and Addictions and the Provincial Health Services Authority may disclose personal information outside Canada:
    a. For the purposes of communicating with individuals respecting COVID-19;
    b. For the purposes of supporting a public health response to the COVID-19 pandemic; or
    c. For the purposes of coordinating care during the COVID-19 pandemic.

    The work included under these purposes may include collaborating between healthcare providers; managing staff, healthcare workers and resources; and carrying out other activities required to deliver ongoing healthcare and related services where these activities are undertaken as a result of the COVID-19 pandemic.

2. Public bodies, including ministries, may disclose personal information outside Canada using **third-party tools and applications** if:
    a. The third-party tools or applications are used to support and maintain the operation of programs or activities of the public body;
    b. The third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g. social distancing, working from home, etc.); and
    c. Any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body. [*In other words, employees should only include personal information that is needed to get the job done.*]

In addition, certain conditions must be met before disclosing personal information outside Canada:

    a. The third-party application must be **reasonably secure**; and
    b. The public body makes all reasonable efforts to remove personal information from the third-

What is a third-party application or tool?

Third-party tools and applications enable communication or collaboration between individuals and include any software developed and maintained by a third party.

What does "reasonably secure" mean?

"Reasonably secure" means that the security measures in place should be in proportion to the sensitivity of the information. For example, health information is more sensitive than an individual's opinion of the weather. Therefore, it would be reasonable for one to expect that health information would be protected to a higher degree.

party application as soon as is operationally reasonable, and the public body retains and manages the information, as required by law.

Implications for B.C. public bodies

Risk Assessments

While Ministerial Order M431 is in effect, B.C. public bodies' other requirements under policy and legislation remain the same. Public bodies should work with their IM/IT, privacy and security experts to ensure that tools are appropriate for use.

The Office of the Chief Information Officer's Privacy, Compliance and Training Branch developed a corporate PIA that assesses risks in government-wide use of third-party applications and tools where this use aligns with the conditions set out in the ministerial order.

Some activities may require different assessments and ministries should work with their Ministry Privacy Officer (MPO) and Ministry Information Security Officer (MISO) to help with this. Broader public sector bodies should work with their internal privacy and security experts to understand and meet their organization's specific requirements.

Additional Responsibilities

Use of third-party applications or tools for communication and collaboration have specific responsibilities. Public bodies must:

- **Make every reasonable effort to remove personal information from the third-party application or tool as soon as possible, and as soon as it is no longer needed.**

  For example, some applications allow you to turn off message history, which deletes content as soon as the application is closed. Other applications allow you to delete content manually once it has been created. Check the Settings of the application or tool you decide to use to determine how to remove personal information.

- **Continue to retain and manage information, as normally required by law.**

  Keep in mind that records management legislation, regulation and policy still applies and that the *Information Management Act* requires ministries and designated public sector organizations to hold, transfer, archive and dispose of information in accordance with an information schedule (e.g., ministries use ORCS and ARCS).

For more information

- **B.C. Privacy and Access Helpline**

  privacy.helpline@gov.bc.ca
  250-356-1851
  Toll-free- Service BC: 1-800-663-7867

- **For Ministries: Information Security Branch**

  InfoSecAdvisoryServices@gov.bc.ca