MINISTRY OF HEALTH: Administrative Health Data Access Suspension Guidelines

1. Purpose

The Administrative Health Data Access Suspension Guidelines (the "Guidelines") are intended to support decision making about the suspension of access to Administrative Health Data ("Data") at the Ministry of Health (the "Ministry"). In addition, the Guidelines provide clarification regarding the roles, responsibilities and accountabilities related to the decision making process.

2. Background

The Ombudsperson's Report, *Misfire: The 2012 Ministry of Health Employment Terminations and Related Matters,* was presented to the Speaker of the Legislature in April 2017. The Report included 41 recommendations. Recommendation 24 is as follows:

> *"By December 31, 2017, following consultation with the Information and Privacy Commissioner, the Ministry of Health create new guidelines for making decisions about suspending access to administrative health data. The guidelines should address the flaws in ministry practice that we identified in this report including better defining the threshold for data suspensions in cases where there is only an unconfirmed suspicion of a data breach."*

The Ombudsperson identified a number of flaws in the decision making process to suspend access to Data by individual employees and contractors, including:

1. The initial reviewer did not have the necessary training or experience to undertake the review and did not consult with anyone with subject matter knowledge relevant to the complaint;
2. During the initial review of the complaint there was a failure to clearly distinguish whether the purpose of review was to clarify or evaluate the complaint;
3. There was a lack of effective oversight for the investigation and the lead investigator's role and reporting relationships were unclear;
4. There was insufficient evidentiary basis for the decisions;
5. In a number of cases, the Ministry failed to notify individuals that their data access had been suspended, did not provide reasons for the suspension, and did not provide the individuals with an opportunity to respond to the allegations against them;
6. The investigation was not conducted in a timely way and, as a result, the suspensions went on for much longer than was reasonable or necessary; and
7. The Ministry did not adequately consider the impacts of many of the data access suspensions on health research and whether and how those impacts could be mitigated or addressed.

3. Guiding Principles

The Guidelines are based on the following principles:

- Suspending Data access based on conjecture or mere suspicion, in the absence of any evidence, is inappropriate.
- Decisions to suspend access to Data should be documented, with relevant reasons and supporting evidence clearly set out.

- A person whose access to Data is to be suspended should be provided with notification and the opportunity to respond before access is suspended, except in urgent cases where there is believed to be a risk of harm if access is not suspended immediately.
- Investigations, decision making, and related pre- and post-decision activities, should be carried out in a timely manner.
- Access suspension should be reassessed if there are changes in relevant facts or circumstances under which an original decision was made.
- There should be clear accountability within the Ministry for decisions to suspend access to Data.

4. Scope

These Guidelines apply to decisions about suspending access to Data that contains personal health information, including de-identified Data, in the custody/control or ownership of the Ministry. They apply to urgent situations where access is suspended pending the completion of a full investigation (provisional suspension) and situations where access is suspended permanently following the completion of a full investigation.

These Guidelines do not apply to decisions about suspending health care provider access to PharmaNet to provide health services to, or to facilitate the care of, an individual whose personal information is being accessed. Such decisions are addressed within the Information Management Regulation under the *Pharmaceutical Services Act*.

5. Definitions

In these Guidelines:

Access Decision Maker	"Access Decision Maker" means the Assistant Deputy Minister of the Health Sector Information Management and Technology Division, or other responsible Ministry official as assigned by the Associate Deputy Minister responsible for Corporate Services ("Associate"). If the Access Decision Maker believes they lack sufficient capacity, training, knowledge, authority, objectivity or experience necessary to competently assess the evidence and make a decision to suspend access, the Access Decision Maker must advise the Associate, who will assign an alternative Access Decision Maker.
Administrative Health Data	"Administrative Health Data" is health information generated through the routine administration of health care programs.
Information Incident	"Information Incident", as defined in the *Information Incident Management Process (IIMP)*, means a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.[1] Information Incidents include Privacy Breaches.

[1] URL: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents

Privacy Breach	"Privacy Breach", means that the collection, use, disclosure, access, disposal or storage of Data containing personal information, whether accidental or deliberate, is not authorized by the *Freedom of Information and Protection of Privacy Act.* For the purpose of these guidelines, "Privacy Breach" also includes the collection, use, disclosure, access, disposal or storage of Data containing personal information, whether accidental or deliberate, not authorized by an applicable enactment such as the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, the *Medicare Protection Act*, the *Laboratory Services Act*, or the *Pharmaceutical Services Act.*[2]

5. Roles and Responsibilities

Ministry Staff

- The Core Policy and Procedures Manual and the IIMP require Ministry staff and contractors to report any actual or suspected Information Incident immediately to their supervisor, the Ministry's Chief Information Officer (MCIO) and the Corporate Information and Records Management Office (CIRMO), by calling the Shared Services Client Service Centre at 250-387-7000.

Corporate Information and Records Management Office (CIRMO)

- A CIRMO investigator with an appropriate amount of training and experience will be assigned to conduct the investigation.
- The CIRMO investigator will consult with relevant Ministry personnel and will make recommendations, as appropriate, to the Ministry relating to the possible suspension of a person's access to Data.

Associate Deputy Minister responsible for Corporate Services ("Associate") Ministry of Health

- In circumstances where an Access Decision Maker is unable, or has been found unsuitable, to perform their role and duties, the Associate will assign a substitute Access Decision Maker.
- Reviews reports from the Access Decision Maker respecting decisions to suspend access to Data pursuant to this Guideline.
- Reviews appeals once investigation is complete and decision to suspend access is finalized.

Access Decision Maker

- Satisfies him or herself that the available evidence justifies any decision related to the suspension of access to Data.
- Makes and documents decisions regarding the suspension of access to Data.
- Considers a person's response to notification in final decision to suspend access.
- During an investigation, reviews appeals of a provisional suspension when investigation does not conclude in a reasonable timeframe.

---

[2] A "Privacy Breach" is referred to as a "Data Breach" in the Ombudsperson's Report.

6. Guidelines for Suspending Access to Data

Identification of Possible Privacy Breach

A complaint, an audit or unusual/irregular access as identified through logging and monitoring can trigger an investigation of a possible Privacy Breach.

Investigation Process

Following the report of an Information Incident, a CIRMO investigator will be immediately assigned to initiate an investigation. The CIRMO investigator will lead an investigative team along with Ministry staff, including representation from the impacted business area and the Ministry Information Security Officer.

The investigative team will report to the Ministry Chief Information Officer and Ministry Chief Privacy Officer.

Where the possibility of a Privacy Breach is identified, the investigative team led by the CIRMO investigator should interview relevant parties that may include:

- The Complainant;
- The person(s) whose access is being investigated, where appropriate;
- System vendors and/or data managers;
- Relevant Ministry program areas;
- Health sector parties, including Health Authority staff;
- The police, where appropriate, as per Ministry of Justice's procedure for reporting misconduct in non-emergency situations;
- Any third-party security/audit service provider, or other body having a legitimate role in any investigations, mitigation activities, etc. where relevant/applicable;
- The Public Service Agency, where the Privacy Breach and the contemplated suspension of access to Data relates to a person appointed under the *Public Service Act;* and
- Other persons of interest.

The investigative team will:

- Thoroughly document all evidence supporting a suspected or actual Privacy Breach, or supporting the absence of a Privacy Breach, gathered during the investigation.
- As appropriate based on the consideration of evidence identified and the urgency of the situation, prepare Interim Reports for the Access Decision Maker that recommend, at any stage of the investigation:
    - The suspension of access to Data on provisional basis where the evidence identified, if true, could support a conclusion that Data may be misused or disclosed improperly; or
    - The overturning of a decision to suspend access on a provisional basis where evidence subsequently identified suggests that the risk associated with continued access to Data while the investigation is underway is acceptable.
- During the course of the investigation, document in writing both (1) the evidence on which any recommendation is based and, (2) the reasons for any access suspension recommendation.
- At the completion of the investigation, prepare a Final Report for the Access Decision Maker that recommends whether or not to suspend access to Data on permanent basis, and

documents all relevant evidence, including any risks or implications associated with a possible Privacy Breach.

- The Final Report, and any Interim Report to a lesser degree of comprehensiveness, should demonstrate that the investigative team has considered:
  - If it is reasonable to conclude that the Information Incident may potentially cause moderate or serious risk of harm to a member of the public, the Ministry, an employee, a contractor or any other person;
  - Whether there is reason to believe that the person acted with malice or ill intent, intentionally and knowingly initiating or facilitating a Privacy Breach;
  - That suspension of access will prevent harm;
  - That there is reason to believe that not suspending or restricting the person's access will result in further breach activity and potentially harm to individuals;
  - The impact of the suspension to the person whose access is being suspended and other parties;
  - The business context for which the data was being used and the data access arrangements for the person concerned; and
  - Mitigation strategies that reduce the impact to the person whose access is being suspended including, restricting the person's access, creating a new account or provisional suspension until further evidence is identified.

Access Decision

- When deciding whether to suspend access to Data, the Access Decision Maker should consider the requirements of any enactments and/or agreements that might apply in the specific circumstances.
- The Access Decision Maker should only suspend access to Data when provided with sufficient reliable, credible and relevant evidence on which to base a decision. An Access Decision Maker may request more evidence or information from the investigative team prior to making a decision to suspend access.
- Where an Interim or Final Report recommending suspension (provisional or permanent) of access is provided, the Access Decision Maker should assess the justification and document his or her decision within reasonable timelines.
- In urgent situations where there is believed to be a risk of harm if access is not suspended immediately, a decision to provisionally suspend access is time-sensitive and should be made as soon as practicable. A permanent decision should normally be made within one week of the receipt of the Final Report.
- A provisional decision to suspend access should be reassessed by the Access Decision Maker:
  - At any time during an investigation upon the receipt of any additional Interim Reports, and
  - At the completion of the investigation upon the receipt of the Final Report.
- When the Access Decision Maker has decided to suspend a person's access following an actual or suspected Privacy Breach, the decision maker should provide their report and decision to the Associate as soon as practicable.

Notification of a Suspension of Access

Provisional Suspension

- The Access Decision Maker should notify a person of a decision to provisionally suspend access to Data prior to suspending access except where there is reason to believe that such notice may result in further breach activity and potential harm to individuals.
- Provisional suspension may occur at any stage of the investigation and any party whose access has been suspended on a provisional basis should be provided with a summary of the evidence supporting a provisional suspension and given an opportunity to respond to the decision.

Permanent Suspension

- At the conclusion of an investigation, the Access Decision Maker should provide a meaningful opportunity for the person to respond prior to making a final decision to suspend access. In doing so, the Access Decision Maker should:
    - Provide the person with a written summary of the reasons and basis for the decision supporting the proposed suspension decision;
    - Provide the person an opportunity to respond in writing to the Access Decision Maker within fourteen days, or further time as the Access Decision Maker determines is reasonable, of being provided notice.
    - Address any matters raised by the person in their response in written reasons for the final decision.
    - Deliver written reasons for the final decision to the person and advise them of their ability to appeal the final decision to the Associate within 30 days of receipt.

Timeliness and Report to Associate

- The investigation of an Information Incident related to an actual or suspected Privacy Breach should be completed in a reasonable timeframe.
- Where an investigation cannot be completed within 90 days, a reasonable timeframe for completion should be proposed to and approved by the Associate by Access Decision Maker. Any subsequent proposed changes to the completion timeline should be approved by the Associate Deputy Minister.
- Approved investigation timelines, and subsequent approved changes to approved timelines, should be communicated to any person whose access may have been provisionally suspended.
- A decision to provisionally suspend access to Data may occur at any time in the course of an investigation. Access may be re-instated at any time if the basis for suspension is determined to be invalid.
- A person whose access has been provisionally suspended may appeal to the Access Decision Maker if the investigation does not conclude within the approved timeframe.

Appeal

- A person may appeal the final decision of a suspension of access to the Associate in writing within 30 days of receiving the Access Decision Maker's final decision.