College of Veterinarians of British Columbia

CVBC Risk Assessment and Privacy Breach Investigation Policy

Published December 2023

Preamble

Privacy management programs are vital to ensuring public bodies are accountable and transparent with respect to their management of personal information. They promote trust by assuring information sharing partners and the public that the public body is protecting the personal information in its custody or under its control.

Risk Assessment and Investigation

The Chief Information Officer and/or in house legal counsel will initiate an investigation and risk assessment of any privacy breach that may occur at that CVBC. The investigation and risk assessment will include the following:

- Summary of the privacy breach: what information was shared, when and to whom
- Investigation findings:
    - Was the breach in relation to a failure to follow established protocols?
    - If this was a breach of established protocols, please describe the expected protocol as well as the deviation from the protocol.
    - Is there an absence of protocol for the incident that occurred?
    - Has the individual involved completed the required privacy training? https://mytrainingbc.ca/FOIPPA/
- Risk Assessment: Generally speaking, the more sensitive the data, the higher the risk. The Office of the Privacy Commissioner for British Columbia requires a review of what purposes the data could be used for:
    - Could there be harm to physical safety?
    - Could there be identity theft of fraud?
    - Could there be a lost of employment opportunities?
    - Could there be hurt, humiliation, damage to reputation or relationships?
        - Examples of sensitive data, as provided by the Office of the Privacy Commissioner for British Columbia, include health information; government pieces of identification such as social insurance numbers or health care numbers; or financial information such as credit card or debit card numbers

        - Be mindful of sensitivity and context of the information involved
    - Can the breach be contained?
    - Is there a relationship between the recipient of the breach and the individual whose information was breached?

- Risk Mitigation and Prevention:

The CVBC takes all privacy breaches very seriously and takes steps to prevent them from happening again. The following recommendations were developed to address a privacy breach and to prevent similar privacy breaches from happening again:

- Recommendations:
    1) Identify suggested measures to address the breach:
        a. training of the staff member
        b. training and briefing of all staff
        c. policy or process updates
        d. new policy or process development
        e. address any cyber security deficiencies that have been identified
    2) Identify the Assessed Level of Risk based on the investigation and risk assessment process.

Next Steps

The completed investigation and risk assessment report will be reviewed by the Chief Information Officer and the Registrar for action.

If the incident is assessed as high risk to cause significant harm, notifications will be made to the individuals involved as well as the Privacy Commissioner.

Notification:

Effective February 1, 2023 public bodies must:

- Notify individuals and the Office of the Information and Privacy Commissioner when there has been a privacy breach that could result in significant harm such as identify theft or financial loss.
- As a matter of best practice, the CVBC will assess the potential harm that may result from any privacy breach in determining whether notification should be made. If a privacy breach is reasonably expected to cause significant harm, the CVBC will notify the affected individual(s) and/or the Privacy Commissioner for British Columbia.
- Notifications will need to be made without unreasonable delay
- Notifications must be sent in writing to affected individuals and must include:
    - the name of the public body;
    - the date on which the privacy breach came to the attention of the public body;
    - a description of the privacy breach including, if known,

- the date on which or the period during which the privacy breach occurred, and
- a description of the nature of the personal information involved in the privacy breach;
- confirmation that the commissioner has been or will be notified of the privacy breach;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
- a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Notification must be sent to the Privacy Commissioner in writing and must include:

- the name of the public body;
- the date on which the privacy breach came to the attention of the public body;
- a description of the privacy breach including, if known,
- the date on which or the period during which the privacy breach occurred,
- a description of the nature of the personal information involved in the privacy breach, and
- an estimate of the number of affected individuals;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual

The online privacy breach report form for submission to the Privacy Commissioner can be found here

A privacy breach checklist can be found here.

Tracking and Reporting

Every privacy breach regardless of the assessed level of risk will be tracked by the Chief Information Officer and an annual report will be provided to the Registrar with any recommendations for the implementation of continuous improvement.

Low risk privacy breaches will be reported to the CVBC Council at the next regularly scheduled Council meeting, high risk breaches will be reported to the CVBC Council immediately.