Privacy Breach and Complaint Protocol

Effective: December 31, 2012

Approved by: Leo McKenna, CFO

1.0 General

- Privacy breaches and privacy complaints will be handled in accordance with this protocol.
- This protocol is divided into two parts. It will assist staff and management in their response to:
    - Their discovery of a confirmed privacy breach; and
    - A complaint about the handling of the information we collect (including an alleged privacy breach).

2.0 Definitions

"Personal information," as defined in FOIPOP, is recorded information about an identifiable individual. This includes:

- the individual's name, address or telephone number,
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- the individual's age, sex, sexual orientation, marital status or family status,
- an identifying number, symbol or other particular assigned to the individual,
- the individual's fingerprints, blood type or inheritable characteristics,
- information about the individual's health-care history, including a physical or mental disability,
- information about the individual's educational, financial, criminal or employment history,
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else.

A "privacy breach", for the purposes of this protocol, occurs when personal information is accessed or disclosed by the WCB or a WCB service provider to a person or entity (either accidentally or intentionally) that is not authorized to receive the information. A privacy breach may be discovered by a WCB staff member or an external party.

A "privacy complaint" means a concern expressed by a WCB employee or an external (non-WCB staff or management member) individual or organization/agency/company about the WCB's handling of the information we have collected to administer the *Workers' Compensation Act*. A privacy complaint, as part of the investigation, may result in the discovery of a privacy breach.

For the purposes of this policy, the term "Manager" refers to an employee's immediate superior and includes the position titles "Manager", "Director" and "Vice President."

3.0 Is it a Privacy Breach?

The WCB is permitted by law to disclose the personal information of injured workers (without their consent) to a person or entity other than the worker under specific circumstances, as we administer the *Workers' Compensation Act*. In some instances, another law, such as the *Income Tax Act*, may require that we release personal information. Refer to *Authorized Release of Injured Worker Personal Information* for an overview of the circumstances under which the WCB can disclose injured worker personal information.

Privacy breaches most commonly occur when personal information about a worker is lost, or disclosed (mistakenly or purposely) outside the requirements of the law. Privacy breaches may be accidental or intentional; they may be a one-time occurrence or due to on-going problems such as a faulty procedure or technical glitches. Refer to *Tips for Identifying a Privacy Breach* for examples of breaches and tips for identifying a privacy breach.

4.0 Accountability

- WCB employees are required to follow this protocol.
- WCB employees who are involved in the engagement of external agents or contractors by the WCB are accountable for advising these parties that any breach or potential breach of personal information must be immediately reported to the WCB.
- Managers are responsible for ensuring employee compliance with this protocol.

5.0 Privacy Breach Protocol Steps

The Privacy Breach Protocol is made up of 4 steps:

Step 1. Breach Identification and Retrieval
Step 2. Investigation and Containment
Step 3. Notification – Affected Parties
Step 4. Follow-up and Long-Term Action

Ideally, the Privacy Breach Protocol steps will be followed in sequence (refer to diagram in Appendix A). However, it is recognized that circumstances/factors may dictate that some be carried out simultaneously or out of sequence. Management is encouraged to consult with the WCB Legal Counsel (FOIPOP Administrator) or their designate for advice/counsel as required when carrying out their responsibilities as described in this document.

Step 1. Identification and Retrieval

- The staff member who discovers the potential breach must immediately complete the Initial Breach Report section of the *Privacy Breach Report Form*, providing as much information as possible about the nature and extent of the breach. When possible, s/he will initiate retrieval of the information (see operational procedure *Retrieval of Disclosed Documents*).
- The staff member will forward the partially completed Privacy Breach Report Form to the appropriate manager for investigation. Generally, the manager of the unit where a breach occurred and/or where a relationship exists with the individual whose privacy was breached, will be responsible for investigation.
    - If the incident involves claim information, the manager of the unit where the claim currently resides will typically be responsible for investigation. An exception will

be when the claim involved has been profiled to another unit in the time between the breach occurring and discovery (e.g., breach incident occurred in the ISC and the claim has since been assigned to a case worker; breach incident occurred in an IST/WST and the claim has since moved to HEB).
    - If the incident involves assessment-related information that includes injured worker personal information (e.g., Experience Rating Statement, Monthly Advice Notice), the manager of Account Management will typically be responsible for investigation.
    - If the incident involves a WCB employee's claim information, the manager of the unit where the claim is being managed will typically be responsible for investigation.
    - If the incident involves a WCB employee's personal information (non-claim related), the manager of the employee's unit/department will typically be responsible for investigation, with assistance from the Human Resources Department as required.
    - If the staff member who discovers the potential breach does not initially have enough information to determine that a breach occurred AND which department should take responsibility for investigation, the staff member will forward the Privacy Breach Report Form to his/her own manager.

Step 2. Investigation and Containment

- The manager is responsible for investigating the breach and documenting it on the Privacy Breach Report Form. In general, the objective of an investigation is to ensure the immediate requirements of containment and retrieval have been completed and to facilitate any immediate and/or longer term remedial or preventative actions.
- See the *Privacy Breach Investigation Guide* for guidelines on how to carry out an investigation and the level/depth of investigation that may be appropriate. Managers should direct questions regarding the type of investigation that should be carried out to the WCB Legal Counsel (FOIPOP Administrator) or their designate.
- Managers are responsible to make every effort to complete the investigation and forward the Privacy Breach Report Form (Initial Breach Report and Manager's sections completed) to Legal Services within **5 business days** of becoming aware that the incident occurred.
- In some cases, it may be appropriate to inform and/or involve other internal WCB parties in the investigation (e.g., other managers, senior management, Communications, Legal Counsel). If the investigating manager believes that others in the organization may be impacted by the incident, s/he will contact Legal Counsel (FOIPOP Administrator) or their designate as soon as possible for advice on who should be involved/aware of the breach incident and/or contribute to WCB's response.

Step 3. Notification - Affected Parties

- The general rule is that specific individuals impacted by a privacy breach will be notified by the manager of the privacy breach investigation as soon as possible, regardless of the type of personal information disclosed.
- Impacted individuals will be notified by phone, followed by a letter (see *Guidelines for Advising Individuals of a Privacy Breach*). If the affected individual is an injured worker, a Contact Sheet can be completed on E-file to record notification call(s) although the

information recorded should be minimal and must not make any reference to any other individuals (e.g., recipient(s)).
- Ideally, the privacy breach investigation has been completed prior to notification, so the impacted individual can be advised of all actions taken in response to the breach. However, notification may occur sooner if it is determined the potential harm of the breach to the individual may be avoided or mitigated by the individual knowing of the breach as soon as possible.
- In rare instances, it may be appropriate to consider alternative approaches to notification of impacted individuals (see *Guidelines for Advising Individuals of a Privacy Breach*). If the investigating manager believes that direct notification may not be appropriate given the circumstances of a specific incident, s/he will consult with Legal Counsel (FOIPOP Administrator) or their designate as soon as possible for advice on how to proceed with notification efforts.

Step 4. Follow-up and Long-Term Action

Follow-up

- The manager will implement remedial actions (or seek approval to implement if required) identified as a result of the investigation in an effort to prevent further privacy breaches.
- WCB Legal Counsel (FOIPOP Administrator) or their designate will
    - verify that all steps in the protocol have been carried out.
    - review the Privacy Breach Report Form to determine if the Privacy Breach Protocol has been followed. If deficiencies are identified, WCB Legal Counsel (FOIPOP Administrator) or their designate will contact the manager to discuss the deficiencies with a view to improved future reporting and management of privacy breaches.
- The WCB Legal Counsel (FOIPOP Administrator) or their designate will, using the Privacy Breach Incident Risk Assessment Tool, assign a risk level to the privacy breach incident for tracking and reporting purposes.

Long-Term Action

- WCB Legal Counsel (FOIPOP Administrator) or their designate will, on a Quarterly basis, compile the information contained in Privacy Breach Report Forms and provide a Privacy Breach Trend Report to the Privacy Advisory Committee (PAC). The report will include charts and trend analysis of breach volumes by various dimensions (e.g., department, risk level, root cause). The report may also include:
    - Observations and details of specific incidents in order to provide context to the statistics;
    - Information and/or trend analysis around privacy complaints (see Section 6.0 below).
- The Privacy Advisory Committee will review the report with the intent of identifying trends and root causes that will ultimately help prevent future breaches and improve organizational privacy practices. The Committee will develop advice or suggestions for further, longer-term organizational actions based on findings and observations supported by the Privacy Breach Trend Report and submit to senior management for consideration and/or prioritization.

6.0 Privacy Complaint Process

WCB employees may receive a call or letter from a citizen or another WCB employee:

- complaining of an alleged breach of that person's personal information;
- complaining that they have received someone else's personal information in error;
- expressing a general concern about the WCB's handling of the information we collect.

This is a privacy complaint. It may be determined, upon initial or more in-depth review, a privacy breach has occurred. In these instances, the WCB Privacy Breach Protocol (above) will be used.

Step 1. Receive and Document the Complaint

- When a complaint is received by telephone or in person, discuss the details of the complaint with the complainant and document what the complainant believes has happened.
- When a complaint is received by e-mail or letter, or once the details provided to you in person or by phone have been documented, forward the complaint to your manager.
- If the complaint is an injured worker complaining they have received the personal information of another injured worker, use the Privacy Breach Protocol (above) and discontinue use of the Privacy Complaint Process.
- NOTE: Documentation of privacy complaints must NOT be added to a claim file (i.e., on E-file). This will help to prevent any misperception that claim adjudication may be affected by initiating a complaint.

Step 2. WCB Response Coordination

- The manager will report the complaint to the WCB Legal Counsel (FOIPOP Administrator) or their designate.
- Complaints received by the Client Relations Officer may be sent directly to the WCB Legal Counsel (FOIPOP Administrator) or their designate, instead of first going to a manager.
- WCB Legal Counsel (FOIPOP Administrator) or their designate will be responsible for the WCB's response and decide who within the WCB should be notified.

Step 3. Investigation and Communication with the Complainant

- The WCB Legal Counsel (FOIPOP Administrator) or their designate will:
    - Send written acknowledgement to the complainant, restating the details presented by the complainant.
    - Contact the complainant as soon as possible, but no later than 30 days of receiving the complaint, and advise them:
        - They may need to contact the complainant for more information as the investigation progresses discuss the complaint with other in the WCB to fully understand the complaint.
        - They may also need to get in touch with other people to fully understand the complaint and this could require the mention of the complainants name and some of the details of their personal information as part of the investigation.

        - If the privacy complaint is about the conduct of one or more WCB employees, the matter will be discussed with the staff members(s) during the investigation.
    - If necessary, send a written update of progress of the investigation (stage of investigation, follow-up activities, expected or updated time-frames etc.). This will be done after no more than two months has elapsed since the initial acknowledgement of the complaint.
    - Produce an investigation report. The report will, at a minimum, include:
        - A summary of the initial complaint.
        - The outcome of the complaint (substantiated/not substantiated).
        - Documentation of the investigative process and findings.
        - Mitigating activities.
        - Other follow-up activities.
    - Communicate a summary of the final results of the investigation to the complainant.
    - Advise the complainant that they may contact the WCB's Client Relations Officer if they are not satisfied with the WCB's investigation. The Client Relations Officer is required to follow Policy 10.3.1R – Quality of Service Delivery and will review the WCB's investigation of the privacy complaint to determine if the WCB followed appropriate processes in handling the complaint. The Client Relations Officer will contact the complainant with the results of their review.
    - Advise the complainant that if they are not satisfied with the Client Relations Officer's review of their complaint, they may make a complaint to the Office of the Information & Privacy Commissioner of Nova Scotia.