



**Nova Scotia Freedom of Information
and Protection of Privacy Report of Review Officer, Dulcie McCallum**

**P-11-01
Workers' Compensation Board of Nova Scotia
November 18, 2011**

Privacy Matters: Creating a Zero Tolerance Privacy Environment

Index:

1. Introduction
2. Background
3. Privacy in the Context of the WCB
4. Discussion
5. What Witnesses Have Told the Review Office
6. What the WCB Does
7. How the Work of the WCB Relates to this Privacy Investigation
8. What the WCB's Privacy Policy Says and How it is Supposed to Operate
 - a. Levels of a Privacy Breach
 - b. Step 1 of the Privacy Breach Policy: Identification and Containment
 - c. Step 2 of the Privacy Breach Policy: Investigation
 - d. Step 3 of the Privacy Breach Policy: Management of the Breach
 - e. Step 4 of the Privacy Breach Policy: External Notification
 - f. Step 5 of the Privacy Breach Policy: Follow-up and Prevention of Future Breaches
 - g. The WCB Privacy Breach Advisory Committee
 - h. Accountability within the WCB
9. The Practical Application of the Policy
 - a. Inaccurate Classification of Personal Information
 - b. Drawing a Distinction in the Definition of Personal Information
 - c. How the WCB Makes a Determination about the Level of Sensitivity
 - d. Major Privacy Breach Characterized as Minor
 - e. Remedial Action through a Direction to Staff
 - f. The Impact of the Recipient on the Level of Breach
 - g. What Risk is Being Assessed?
 - h. Failure to Provide Notification to Workers
 - i. Changing the Determination of the Breach Level
 - j. The Role of the Privacy Breach Advisory Committee
10. Findings
11. Recommendations
12. The WCB's Response to the Recommendations

1. Introduction

Privacy matters. Among the general public, there is a growing understanding that privacy is a fundamental right and an enhanced appreciation that personal information needs to be protected. In 2009, the Access and Privacy Commissioners of Canada stated, in part, in a joint resolution:

Whereas

1. *Privacy is a fundamental human right that enables the freedom of association, thought and expression.*
2. *Canadian courts have consistently affirmed the importance of these rights.*

Privacy breaches in the public and private sector are frequently headline topics. What the right to privacy entails has attracted considerable media attention and as a result members of the general public are gaining an improved understanding of who bears responsibility to protect their privacy and what obligations result for public officials: to inform, to contain, to remedy and to prevent.

In recent years, the Nova Scotia Legislature has demonstrated its appreciation of the importance of privacy protections. In 2009, the *Privacy Review Officer Act* was proclaimed providing for independent oversight of privacy complaints in the provincial public sector. In 2010, the *Personal Health Information Act* [“*PHIA*”] passed the House of Assembly and is awaiting proclamation. *PHIA* makes provision for similar independent oversight as the *Privacy Review Officer Act* for privacy complaints regarding personal health information. In addition to providing the right to request a Review of an alleged privacy breach, *PHIA* requires public bodies or custodians to provide the Privacy Review Officer with automatic notification of all privacy breaches except where the individuals affected are notified. These legislative protections illustrate the importance government is placing on privacy protection on behalf of its citizens.

Under the powers in the *Privacy Review Officer Act*, the Review Officer initiated this Privacy Review after reports of allegations surfaced that the Workers’ Compensation Board of Nova Scotia [“*WCB*”] may have breached some injured workers’ privacy.

2. Background

On Friday, January 14, 2011, the *Chronicle Herald* reported that an injured worker, after requesting a copy of his claim file from the WCB, received another worker’s file instead. This media coverage sparked a number of calls to the Review Office with individuals reporting similar incidents. By the end of day January 14, 2011, the Privacy Review Officer made a decision to exercise her discretion to initiate an investigation on her own motion, as contemplated by s. 5 of the *Privacy Review Officer Act*.

Review Office staff notified the WCB that the Privacy Review Officer would be opening her own-motion investigation as follows:

[T]he Review Officer will be initiating an investigation into reports that the [WCB] mailed a file containing the personal information of a WCB client to another WCB client.

On Monday, January 17, 2011, the Privacy Review Officer e-mailed the WCB to clarify that this would be a systemic investigation and was not related to one specific individual:

[O]ur own motion investigation is about individuals whose privacy has potentially been breached when their file was shared improperly.

On Tuesday, January 18, 2011, the Privacy Review Officer issued a press release saying:

I became very concerned late last week when stories emerged that workers who had dealings with the WCB had received someone else's personal information in the mail. Our focus will be on those individuals whose personal information may have been shared with another person without their consent or knowledge . . . On Friday I indicated that by early this week I would make a decision with respect to the alleged privacy breaches. Today I confirm that I have notified WCB that based on my new authority under the Privacy Review Officer Act I have initiated an investigation with respect to the allegations reported and others that have surfaced since.

A letter followed from the Privacy Review Officer to the WCB on Thursday, January 20, 2011, outlining the authority for her own motion investigation and the intended procedure:

1. *Section 5 of the PRO Act is the authority for this investigation and reads as follows:*

5 (1) In addition to the Privacy Review Officer's duties and powers referred to in Section 6 with respect to reviews, the Privacy Review Officer may

(b) initiate an investigation of privacy compliance if there are reasonable grounds to believe that a person has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention;

2. *Section 5 is distinct from s. 6 of the PRO Act. Based on that we would be looking at a broad definition of privacy breach. Privacy breach will be defined as when there has been unauthorized access to or disclosure of personal information by WCB in contravention of applicable provincial legislation.*
3. *The Protection of Personal Privacy: Collection, Protection, Retention, Use and Disclosure of Personal Information part of the Freedom of Information and Protection of Privacy Act ["FOIPOP"] is the applicable provincial legislation. Specifically the provisions contained in s. 27 of FOIPOP will define when a public body is entitled to disclose personal information.*

This letter requested the WCB provide the Review Office with the following documents as the starting point for the privacy investigation:

1. *Copies of all of the WCB's existing written internal privacy policies.*
2. *Copies of all of the WCB's existing written internal privacy procedures.*
3. *If the privacy policy is silent on procedures, provide an explanation of the WCB's present practices in response to a privacy breach.*
4. *Copies of all incident reports for the period January 2000 to present that specifically address instances of privacy breaches: that is incidences where the WCB disclosed the personal information of clients to other clients. If the documentation of these*

occurrences is referred to as other than incident reports, please provide copies of that documentation for the period requested.

5. *Copy of the existing WCB notification form [blank] used when notifying individuals of a privacy breach.*

When the WCB replied to this letter on February 4, 2011, it indicated its understanding of the scope of the Privacy Review as follows:

Ms. McCallum . . . indicated the Review Office would be considering a broad definition of privacy breach during this investigation; and that the definition would be: . . . when there has been unauthorized access to or disclosure of personal information by WCB in contravention of applicable legislation.

Six months into the investigation, in a phone call on July 14, 2011, the WCB indicated it had some confusion as to the scope of the Review, suggesting that it was not until much later in the process that it fully understood the scope to be broadly examining the WCB's privacy practices. The Privacy Review Officer's public comments, her direct comments to the WCB, the request for all privacy policies, procedures and incident reports and the WCB's comments in its initial reply letter to the Review Office all indicate that the scope was to be a broad one examining the WCB's organizational privacy practices and that had been made clear from the outset of the investigation.

During the course of the investigation, the following records were examined:

1. WCB's internal Privacy Breach Notifications [The relevant WCB documentation related to this Review variously titles these memos "Privacy Breach Notification," "Privacy Breach Report" or "Interim Privacy Breach Report." For the purpose of this Privacy Review Report, I will use the phrase "Privacy Breach Notification" throughout];
2. WCB Legal Services Responses to Privacy Breach Notifications;
3. WCB Policy B16.1.1, Privacy Breach Policy;
4. WCB Policy 10.3.10, Corporate Information Protection Policy;
5. De-identified copies of WCB Performance Planning and Assessment Documents (PPAs) for WCB staff whose PPA had a goal related to limiting privacy breaches;
6. Internal WCB correspondence related to efforts to mitigate privacy breaches since the beginning of the Review Officer's investigation;
7. *Every Day Forward*, WCB's 2010 Annual Report;
8. WCB Template and SMART Letters and Decisions;
9. The WCB website, www.wcb.ns.ca, and its promotional website, www.worksafeforlife.ca;
10. Privacy Breach Notification memos starting in September, 2008 [however, emphasis was given to those created after the formal Policy became effective in September 2009].

In addition, the following legislation and guidelines were reviewed and considered during the investigation:

1. *Privacy Review Officer Act* ["PRO Act"];
2. *Freedom of Information and Protection of Privacy Act* ["FOIPOP Act"];
3. *Workers' Compensation Act* ["WCA"];
4. *Personal Health Information Act* ["PHIA"] [note not yet proclaimed];

5. *Privacy Breach Guidelines*, Office of the Information and Privacy Commissioner of Saskatchewan.

The Privacy Review Officer acknowledges the efforts made by the WCB to cooperate throughout this Review.

3. Privacy in the Context of the WCB

Work is one of the most important aspects of a person's life. It often defines who we are, how we feel about ourselves, whom we associate with and our sense of achievement. To lose the ability to work, temporarily or permanently, because of a workplace injury can be devastating to the individual and his/her family.

In fact, the WCB demonstrates it is highly cognizant of the self-worth component of working in its public literature. In particular, the "Rod Stickman" videos on the WCB website highlight the dignity, autonomy and satisfaction derived from workers making meaningful contributions to their jobs. The WCB's emphasis on the importance of these values is commendable.

Workers Compensation legislation is intended to create a safety net for workers while they are unable to return to their place of employment due to the disabling impact of their injury. If s/he needs compensation, an injured worker has no choice but to apply for benefits and rehabilitation from the WCB as the law removes the ability to sue the employer. This creates both a dependency and vulnerability.

Most workers who require WCB benefits are already at a serious disadvantage because they are injured. While in this state of being disabled from working, they are required to make an application for benefits by providing sufficient medical information to substantiate the extent of the injuries that will quantify their claim. The exchange of a significant amount of personal information, particularly personal health information, between the injured worker, his/her health care providers, his/her employer and the WCB is at the core of the benefits process. An injured worker has no choice about this: the legislation requires his/her personal information must be provided to the WCB. The legislation also gives the injured worker a right to a copy of his/her personal information collected by the WCB, subject to one exception, which is not relevant in this Review.

Workers have to give up their personal privacy – i.e. a fundamental part of themselves, their dignity, and their ability to be autonomous – to the WCB in the course of pursuing a claim and return to work. Privacy is as important in achieving an individual's dignity, autonomy and self-worth as a steady job. In helping workers back to work, or assisting those who can never go back, the WCB needs to be cognizant of the self-value of privacy.

This Review Report is about the privacy policy and practices at the WCB in relation to one aspect of how it manages the personal information it collects and discloses about injured workers.

4. Discussion

The *PRO Act* authorizes the Privacy Review Officer to initiate an investigation of a public body if there are reasonable grounds to believe there has been a contravention of a privacy provision.

5 (1) In addition to the Privacy Review Officer's duties and powers referred to in Section 6 with respect to reviews, the Privacy Review Officer may

(a) monitor how the privacy provisions are administered and conduct reviews of privacy complaints arising from the privacy provisions;

(b) initiate an investigation of privacy compliance if there are reasonable grounds to believe that a person has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention;

(c) make recommendations on and mediate privacy complaints;

(d) undertake research matters concerning privacy legislation;

(e) inform the public about this Act;

(f) on the request of a public body, provide advice and comments on privacy.

[Emphasis added]

Unlike where a privacy complaint is received requesting a Review, in a self-initiated investigation, the Review Officer is ***not required*** to ensure those affected have completed the use of the public body's internal privacy-complaint mechanism.

5(2) The Privacy Review Officer may only exercise the powers under clauses (1)(a) and (c) after the person who has made the complaint has completed the use of the internal privacy-complaint procedure of the public body to which the complaint was made.

In this case, those individuals who came forward after the Review was publicly announced were not asked by the Review Office to submit a complaint to the WCB. In addition, no individual privacy complaint files were opened at the Review Office for these individuals and their information was received on a confidential basis. Confidentiality has been strictly maintained as some of the individuals who came forward feared retribution in the claim process if they were identified.

The *FOIPOP Act* gives public bodies such as the WCB the discretion whether or not to disclose personal information but only in the circumstances listed in s. 27 of the *FOIPOP Act*, which reads as follows:

Disclosure of personal information

27 A public body may disclose personal information only

(a) in accordance with this Act or as provided pursuant to any other enactment;

(b) if the individual the information is about has identified the information and consented in writing to its disclosure;

- (c) for the purpose for which it was obtained or compiled, or a use compatible with that purpose;*
- (d) for the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment;*
- (e) for the purpose of complying with a subpoena, warrant, summons or order issued or made by a court, person or body with jurisdiction to compel the production of information;*
- (f) to an officer or employee of a public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;*
- (g) to a public body to meet the necessary requirements of government operation;*
- (h) for the purpose of*

- (i) collecting a debt or fine owing by an individual to Her Majesty in right of the Province or to a public body, or*
- (ii) making a payment owing by Her Majesty in right of the Province or by a public body to an individual;*

- (i) to the Auditor General or any other prescribed person or body for audit purposes;*
- (j) to a member of the House of Assembly who has been requested by the individual, whom the information is about, to assist in resolving a problem;*
- (k) to a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;*
- (l) to the Public Archives of Nova Scotia, or the archives of a public body, for archival purposes;*
- (m) to a public body or a law-enforcement agency in Canada to assist in an investigation*

- (i) undertaken with a view to a law-enforcement proceeding, or*
- (ii) from which a law-enforcement proceeding is likely to result;*

(n) if the public body is a law-enforcement agency and the information is disclosed

- (i) to another law-enforcement agency in Canada, or*
- (ii) to a law-enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;*

- (o) if the head of the public body determines that compelling circumstances exist that affect anyone's health or safety;*
- (p) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted; or*
- (q) in accordance with Section 29 [research] or 30 [archives]. 1993, c. 5, s. 27 .
[Explanation added]*

Section 27 of the *FOIPOP Act* does not authorize the WCB to release one injured worker's personal information to another injured worker. I find the disclosure of the personal information constitutes a privacy breach under the *FOIPOP Act*. I find that the WCB acknowledges it had no

authority to disclose the personal information in the manner that is subject to this Review. While there was no evidence the releases were intentional, malicious or purposeful, the breaches remain serious.

This Review Report will not make any finding that lays fault at the feet of any one person be he or she a caseworker, a manager, a director or an assistant. The root causes of the problem will not be solved by blaming particular individual employees and I will not engage in any discussions that would lead to identification of any one person that may result in sanction or retribution.

5. What Witnesses Have Told the Review Office

When the Review Officer first gave notice that she was considering her own motion investigation, the Review Office invited individuals who may have received another injured worker's personal information to come forward with their stories. Twelve individuals contacted the Review Office in total [four of whose complaints were from the time period after the Privacy Breach Policy was effective] to say that they had received another injured worker's personal information either mixed in with their file, or as a unique record. Many claimed that they knew of others who had similarly received information on another worker. Many witnesses insisted on anonymity out of fear of retribution, particularly those involved in an appeal of a WCB decision that affected their claim.

Although the Review Office has relied almost exclusively on the facts presented in the records provided by the WCB in creating this Review Report, the comments from injured workers have been helpful in providing context to aid the Review Office's understanding of the impact a privacy breach may have on those who rely on WCB for their income. The Review Officer appreciates those who come forward with information.

The WCB requested the names of those individuals who may have had a privacy complaint during this Review. These names were not provided to the WCB because the Review Office promised anonymity to those who contacted our Office. In addition, many of those individuals said they did not want to file a complaint with the WCB as they feared retribution. It is the usual practice of the Review Office to require individuals wishing to file a privacy complaint to first file a complaint with the public body and return to our Office if they remain dissatisfied. However, the nature of a systemic investigation requires a "big-picture" view, rather than the examination of individual complaints. The testimony of those who came forward was helpful and, more importantly, consistent with the investigation of the WCB's records, policy and practices which forms the core of the Review findings and recommendations.

It is worth noting, however, that it is a sad testimony to the work of the WCB if injured workers and their families consider retribution to be a real possibility. This is particularly the case given the WCB has publicly committed to caring and compassion as parts of its core values: *We will strive to walk a mile in workers' and employers' shoes. We will serve as we like to be served and provide those we serve with the respect and support they need to be successful.* By promoting compliance and due diligence under the Privacy Breach Policy ["Policy"] and devoting more attention to the importance of respecting personal privacy, the WCB will take a step towards reaching its stated goal of demonstrating respect and support for injured workers.

6. What the WCB Does

The WCB describes itself as follows:

Funded entirely by the employers of Nova Scotia, the WCB provides workplace injury insurance for more than 18,000 employers, representing about 300,000 workers across the province . . .

The WCB identifies its vision, mission, values and goals as follows:

Our Vision

Nova Scotians – safe and secure from workplace injury.

Our Mission

We set the standard for workplace injury insurance. We inform and inspire Nova Scotians in the prevention of workplace injury, but if it occurs we support those whose lives it touches by championing a timely return to safe and healthy work.

Our Values

Can-do Attitude

We will deliver on our promises and provide top-notch service.

Safety Champion

We will be a champion for workplace safety through our relationships and innovative solutions, and by keeping prevention and return to work at the heart of our business.

Caring and Compassionate

We will strive to walk a mile in workers' and employers' shoes. We will serve as we like to be served and provide those we serve with the respect and support they need to be successful.

Our Goals

- *An unwavering focus on workplace injury prevention.*
- *Helping injured workers and employers plan a safe and timely return to work.*
- *Building confidence in the WCB by engaging workers and employers in creating safer workplaces.*
- *Working with others to expand the commitment to injury prevention and return to work across the province thereby further improving outcomes for Nova Scotians.*
- *Making service improvements to provide workers and employers with a higher level of service tailored to meet their needs – supportive, compassionate service.*
- *Maintaining our strategy to reach full funding and bring financial sustainability to the Workplace Safety and Insurance System.*

In a Representation to the Review Office dated July 28, 2011, the WCB says:

The WCB has always been mindful to protect our stakeholder's information entrusted in our care very seriously. More recently, we have adopted formal policies codifying how this information is protected. All WCB employees have received training with respect to privacy and our legislated obligations; this is also provided to all newly hired staff as well.

7. How the Work of WCB Relates to this Privacy Investigation

The WCB provides “no-fault” insurance for workers injured on the job, to ensure a replacement of earnings lost due to a workplace injury. The WCB places great emphasis on preventing workplace injuries and helping workers transition back to the workplace. From the perspective of individual injured worker’s privacy, the most significant areas are the claims and the return to work processes.

When a worker is injured on the job, his/her employer is required to fill out an injury report and send it to the WCB. The injury report requires the employer to provide the WCB with the injured worker’s name, occupation, address and phone number, as well as his/her Nova Scotia Health Card number, Social Insurance Number [“SIN”], date of birth and gender. The injury report also requires complete details of the injury/illness sustained by the worker and the injured worker’s employment history.

The injured worker is required to notify his/her doctor or health care provider when s/he is first examined following the injury that the injury was sustained at work and will involve a WCB claim. The health care provider then completes and submits an “8/10” form to the WCB detailing the medical analysis of the injury/illness, including “objective” and “subjective” findings and details of the return-to-work and health care treatment plans.

When these reports are received, the WCB opens a claim file. A worker can have multiple claim numbers over the course of his or her life, with one or more claims active at any given time. When the claim file is opened, the Benefits Administrator [“BA”] makes a determination derived from the apparent complexity of the case, which is based on how long an individual is expected to be off work as a result of the injury/illness. The claim file is then assigned to a Caseworker [“CW”].

The CW collects all the relevant information to enable the WCB to make a decision on the level of benefits the injured worker will receive. Once the level of benefits decision is made by the CW, the injured worker has 30 days in which to file an appeal. ***If s/he decides to appeal, the worker must file a notice of appeal, which requires that all documents relevant to the appeal are included with it.*** That means a worker who decides to appeal must submit a request and receive a copy of his/her file within the 30-day window in which an appeal must be filed.

If the worker is unsatisfied with the results of the internal appeal, s/he may then appeal to the Worker’s Compensation Appeals Tribunal [“WCAT”]. If the results of the WCAT appeal are still unsatisfactory, any party including the worker has a statutory right to appeal to the Nova Scotia Court of Appeal.

Section 193 of the WCA gives every injured worker the right to access any record in his/her claim file:

Worker entitled to copy of documents

193(1) Any worker may receive a copy of any document or record in the Board's possession respecting the claim of the worker.

(2) Where the Board has determined that a document or record contains medical information that would be harmful to the worker if released to the worker, the Board may

- (a) release the document or record to the worker's physician; and*
- (b) inform the worker that it has released the document or record to the worker's physician.*

(3) An employer, who is a participant in

- (a) repealed 1999, c. 1, s. 23.*
- (b) an appeal to a hearing officer, may, subject to any procedure that may be adopted by the Board, receive a copy of any document or record in the Board's possession that the Board considers relevant to the appeal.*

(4) No decision, order or ruling of the Board on an issue in which the employer has a direct interest shall be based on any document or record to which the employer has been denied access pursuant to this Section.

(5) Subject to subsection (6), the Board may charge a fee for providing any copy of a document or record pursuant to this Section.

(6) A worker is entitled to one copy of any document or record requested pursuant to subsection (1) without charge where the worker's claim has been denied by the Board. [Emphasis added]

A worker makes a request for his/her information held by the WCB by submitting a form addressed to the photocopy department. The WCB provides workers with one copy of their claim file without charge but may charge for subsequent copies with the exception of any new information being added to the worker's file. There are clearly some time pressures on the photocopy department, as it would be essential that the worker's file be sent to him/her in advance of the 30-day appeal window being closed.

This process is distinct from that of the CWs who frequently send out letters looking to gather more information, informing workers of new information and/or advising about new decisions. They may be sending many, many letters in the course of a day, but they are mostly individual documents, correspondence from the CW addressed one at a time, and frequently copied to employers, health care providers and/or the injured workers themselves.

In the result, there is a significant amount of personal information exchanged back and forth between injured workers, WCB employees including CWs, health care providers and employers. I find that the collection, retention, use and disclosure of personal information makes up a large part of the "industry" of the WCB, which is substantiated by the WCB's claim that it processes about 1.75 million transactions involving "personally identifying information" every year.

8. What the WCB's Privacy Policy says and How it is Supposed to Operate

The WCB's current Privacy Breach Policy ["Policy"] has been effective since September 14, 2009. The Policy states its objectives are to:

- *Define the scope and levels of a Privacy Breach*
- *Clearly communicate a process for managing a privacy breach*
- *Clearly establish accountabilities*
- *Minimize the impact of a breach and take prompt action to minimize future breaches.*

The Scope section outlines to whom the Policy applies and provides as follows:

This policy applies to all employees, contractors and third party vendors of the WCB. Everyone employed by or in the contract of service with the WCB has an obligation to be vigilant when working with personal information (e.g. full name, age, address, contact information, SIN, medical history related to claim.) This policy provides direction for managing breaches of personal information.

The Policy defines personal information as "recorded information about an identifiable individual, e.g. name, address, telephone number," and includes a reference to the Corporate Information Protection Policy 10.3.10. The Corporate policy adopts, in its definition section, the definition of personal information from the *FOIPOP Act*:

- (i) *"personal information" means recorded information about an identifiable individual, including*
 - (i) *the individual's name, address or telephone number,*
 - (ii) *the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,*
 - (iii) *the individual's age, sex, sexual orientation, marital status or family status,*
 - (iv) *an identifying number, symbol or other particular assigned to the individual,*
 - (v) *the individual's fingerprints, blood type or inheritable characteristics,*
 - (vi) *information about the individual's health-care history, including a physical or mental disability,*
 - (vii) *information about the individual's educational, financial, criminal or employment history,*
 - (viii) *anyone else's opinions about the individual, and*
 - (ix) *the individual's personal views or opinions, except if they are about someone else;*

The Policy defines a privacy breach as follows:

***For the purposes of this policy a privacy breach is disclosure of personal information, either accidental or intended, that is not authorized by legislation.
[Emphasis in the original]***

a. Levels of a Privacy Breach

Under the Policy, the level of a privacy breach can be either low risk, moderate/medium risk or major risk. Those risk levels are defined as follows, with examples cited in the Policy:

*Low Risk – a breach that affects one or a limited number of people; **the information is not inherently of a personal nature (e.g. information that would be found on a business card)**; the cause has been identified and breach is not ongoing and there is little harm posed to the individual(s) and the organization.*

Example of a Low Risk Breach:

Sending a document to a customer that contains name, address, claim number of another customer. It's a single document, affecting two customers, therefore it is identified and contained at the instant the breach is known.

*Moderate Risk – a sensitive information breach that affects one or more people; **the information is personal (e.g. beyond basic business card information)** and unauthorized access to it could place the individual(s) at risk, e.g. identity theft; the cause of the breach may still be unknown; and/or there is a greater risk of harm to the organization.*

Example of a Medium [sic] Risk breach:

Sensitive personal information is released about a customer to another customer, e.g. SIN number or psychological profile.

*Major Risk – **a breach of private and sensitive information (e.g. beyond business card)** that affects many individuals; a large volume of personal information that would put an individual at risk; the cause of the breach may not as yet be identified, therefore the breach is still active; high degree of harm to the reputation of individuals and the organization.*

Example of a Major Risk breach:

Our system has been hacked or breached or a laptop [or] non-encrypted device (laptop, Blackberry) is lost or stolen – large volumes of personal information, affecting many customers is open to the public.

[Emphasis Added]

The Policy directs that five specific steps are to be taken when a potential privacy breach is discovered. The five steps are described below.

b. Step 1 of the Privacy Breach Policy: Identification and Containment

The first step is “Identification and Containment.” The employee who becomes aware of a breach (either by breaching the information themselves, or by discovering there has been a breach) is required to report the breach to his/her manager. The manager, in turn, “will make an assessment of the scope of the breach and determine the level of the breach. This assessment will dictate the procedure for investigation and management of the breach.”

Under the first step, “containment is a priority” once the cause of the breach is known. The employee discovering the breach is to “act immediately to ensure the breach is contained by ceasing the action that has resulted in a breach.”

c. Step 2 of the Privacy Breach Policy: Investigation

The second step is “Investigation.” The Manager responsible for the area will lead the process to investigate and document the cause of the breach. Where the cause of the breach is not immediately apparent and there may be other causes, such as hacking of a system, the Manager will involve other areas of interest such as information technology.

Under this directive, the investigation will focus on the following:

- *Scope and cause of the breach*
- *Nature of personal information involved*
- *Degree and risk based on the sensitivity of the personal information*
- *Factors that enhance the impact of the breach*
- *The number of individuals that are affected by the breach*
- *Extent of foreseeable harm to the individual(s) whose information has been breached*
- *Extent of harm to the organization.*

d. Step 3 of the Privacy Breach Policy: Management of the Breach

The third step is “Management of the Breach.” The Policy directive requires the Manager to complete a Privacy Breach report that is then submitted to the Legal Services branch of the WCB for “feedback.” Under the third directive, and based on the results of the investigation stage, “the manager and their immediate supervisor along with Communications, and/or other departments will coordinate a strategy for external notification if necessary.”

e. Step 4 of the Privacy Breach Policy: External Notification

External Notification is the fourth step. It reads in its entirety as follows:

- *In cases of moderate to high level breaches, it may be appropriate to contact the individual(s) whose personal information was the subject of the privacy breach depending on the outcome of the investigation*
- *Individuals should be informed of a privacy breach and the specific information disclosed when there is a significant risk of:*
 - a) *Harm or embarrassment to the individual or company*
 - b) *Public disclosure of the personal or corporate information*
 - c) *Opportunity for malicious use of the personal or corporate information*

f. Step 5 of the Privacy Breach Policy: Follow-up and Prevention of Future Breaches

Step five encompasses “Follow-up and Prevention of Future Breaches” and provides, entirely, as follows:

- *The Manager is expected to provide relevant follow-up information on the status of a breach (if information was recovered, destroyed and results of notification) to Communications, Legal Services and Privacy Breach Advisory Committee*
- *In the case of moderate and high risk breaches, the Privacy Breach Advisory Committee will provide a separate quarterly report debriefing the incident for the Executive Team and the organization – intent is to capture the “learnings” and recommend future preventative actions*
- *Legal Services is responsible to report annual privacy breach statistics to the VP responsible for this area.*

g. The WCB Privacy Breach Advisory Committee

In step five there is reference to the WCB Privacy Breach Advisory Committee, which is described in the Policy as follows:

[C]omprised of managers and employees from various units within the organization. The purpose of this committee is to assess and provide advice concerning privacy breaches within the organization; and when requested by Executive Team, to review action and procedures on specific incidents and breaches.

Representatives from the following business areas will sit on the committee:

*Legal
Communications
Central Services
IST
Health and Extended Benefits
IT
Corporate Development
Internal Appeals*

h. Accountability within the WCB

The final section in the Policy refers to accountability within the WCB. There are two components. First there is one person identified as being accountable for **promoting and implementing** the Policy who is a specific manager within the Legal Department. Second the Directors are named as being responsible for **monitoring compliance** with this Policy.

I find that the WCB has fallen short under its own Privacy Breach Policy. While the promoting accountability and monitoring compliance provisions of the written Policy are mostly adequate,

they are not followed. For the purpose of this section, the WCB has failed to follow its own Policy as follows:

- The designated manager has not reported to the Privacy Breach Advisory Committee as the WCB has failed to constitute the Committee;
- The designated manager is accountable to promote and implement the Policy but has fallen short to ensure it is fully implemented and followed;
- Legal Services is required by the Policy to provide statistics on privacy breaches to corporate but this does not appear to have been done.

The bulk of this Report will now focus on the way the Policy has been implemented, as reported in the WCB's Privacy Breach Notification memos.

9. The Practical Application of the Policy

The WCB's Privacy Breach Policy [outlined above in Part 8] went into effect officially as of September 14, 2009. As such, the bulk of this Privacy Review Report will focus on the way the Policy was interpreted after that date. However, because the WCB was preparing Privacy Breach Notification memos as early as September, 2008, these memos have also been examined in the investigation. By letter dated April 8, 2011, the Review Office requested to see all privacy breach memos relating to "any instance in which a client's personal information was disclosed to a recipient for whom WCB did not have the client's consent to disclose." The WCB provided the Review Office with 155 "Privacy Breach Notifications" responsive to this request.

The Privacy Breach Notification follows a specific template and is divided into sections as follows:

- In the heading section, there is a check box for the "manager's risk assessment," where a breach can be marked as either "Minor," "Moderate," or "Major." Some variations of the template will show "Low," "Moderate" or "Major," and still others say "Minor," "Major" or "Other"
- Action Taken to Contain the Breach
- Notification – Internal Staff Notified? Please explain
- Remedial action taken, if any, to ensure breach does not occur in future
- Manager's risk assessment (Low, Moderate, High, please explain)

In its July 28, 2011 Representation, the WCB explained that it processes close to 1.75 million transactions containing "personally identifying information" annually. In that respect, 155 reported privacy breaches over approximately 32 months is a comparatively small number. The WCB further represents that "[f]ortunately, over 90% of . . . recorded breaches have been assessed as low risk in accordance with our policy."

The evolution of the Policy is consistent with the WCB's statement in its July 28, 2011 Representation that it is "continually reviewing operational processes and attempting to identify system improvements to ensure the potential for a privacy breach to occur is minimized. The WCB's Policy lends itself toward helping us to evolve our business information management practices to continue to provide better service to our customers."

An examination of the records provided by the WCB revealed a number of themes, which are detailed below.

a. Inaccurate Classification of Personal Information

The first section of the Privacy Breach Notification asks the manager for “Details of the Breach.” Usually this includes the dates the information was sent out, who received it and how the WCB became aware of the breach. By definition, the section is intended to provide *details of the breach*.

In many cases, not all the personal information disclosed was accounted for. In many others, a label was used to describe the form, without accurately quantifying the amount of personal information actually contained on the form.

Sometimes the letter sent to the wrong recipient is a form letter. For instance, in a Privacy Breach Notification dated April 14, 2011, the manager reported that the personal information disclosed within the letter was the injured worker’s name, address and WCB claim number. On reviewing the letter [which was incorrectly filed in another worker’s claim file – WCB was unable to determine whether or not this letter was disclosed to the second worker] that was precisely the information contained: the letter was a form letter highlighting and explaining the section of the *Worker’s Compensation Act* that describes a worker’s responsibilities during return to work. The only personal information was the injured worker’s name, address and the WCB claim number.

This was reported and accepted as a minor breach.

The Review Office counted 23 out of the 155 breach memos [15%] that recorded the “Details of the Breach” in this kind of detailed and accurate manner.

However, it is often the case that the Privacy Breach Notification simply identifies a type of document that was disclosed. In 77 of the 155 breach memos [50%], the “Details” section contains a label of the type of information that was sent out that would enable staff familiar with the WCB’s processes to know what type of information was disclosed (for instance, “Form C,” “Hearing Officer Decision,” “SMART” letter).

But this labeling does not appear to lead to careful consideration of the amount and type of personal information actually disclosed. Often, the Privacy Breach Notification says that only the name, address and WCB claim number were included on the type of form that was sent, but does not address the fact that the personal information disclosed includes additional personal information recorded on the form. As a result, many of the Privacy Breach Notifications reveal an incorrect assessment of what “personal information” means under the Policy. For instance, in a memo dated October 19, 2009, the details were reported as follows:

[Staff] sent Form C via fax with treatment approval back to originating clinic; however it was sent to the wrong fax number . . . The fax contained the Worker’s name, Health Card Number, Claim number and date of birth.

In response to questions from the Review Office dated March 24, 2011, the WCB described a Form C as follows: “A Physiotherapist’s Progress Report Form. This form is completed and

provided to the WCB by a physiotherapist for each visit an injured worker has with a physiotherapist.” The WCB appended a blank copy of the Form C.

In addition to space for the worker’s name, health card number, WCB claim number and date of birth, the Form C includes three sections that are to be completed by the health care provider, and which describe the worker’s injury and the physiotherapist’s assessment of the injured worker’s ability to return to work. Those sections are as follows:

“Injury Assessment Information” – This includes a line for “MDA Diagnosis (specify body part),” and a section for “Functional Update (Physical Abilities Report attached)”

“Job Match Summary” – This section is three rows with five check boxes each, asking the physiotherapist to choose whether the worker’s “pre-injury”, present and transitional work capacities are sedentary, light, medium, heavy, or very heavy. Attached to the Form C are definitions of these terms, which are “adapted from The Medical Disability Advisor, Presley Reed, M.D., and LRP Publications; and from the National Occupation Classification.”

“Collaborative Treatment Plan” – Includes columns for Goals, Methodology and the recommended time frame.

Although the actual document disclosed was not attached to this particular Privacy Breach Notification (an issue the WCB has, to its credit, been working to rectify), the context of the comments – that the Form C was “faxed back” to the originating clinic, and that it included “treatment approval” suggest it is likely that the Form C had been filled out completely by the physiotherapist.

To then describe the personal information disclosed as “the Worker’s name, Health Card Number, Claim number and date of birth” seems to fall short of the expectations of the Policy as it does not provide *details of the breach of all the personal information disclosed*.

This was reported and accepted as a minor breach.

Similarly, in a Privacy Breach Notification dated February 7, 2011:

A request for medical information was faxed to the incorrect GPs office . . . The worker’s claim number appeared on the fax. The fax asked questions about the medication that the worker is taking.

The Manager’s Risk Assessment classified the breach as Low because “Only the worker’s name and claim number appeared on the fax.”

In this case, the fax was appended to the Privacy Breach Notification. In addition to the worker’s claim number, the worker’s name was on the fax, as well as the following portions of text:

[Worker’s name] has submitted prescription receipts for [named medication] [dosage] dating back to [date].

At this time, [WCB] requires further medical information from you regarding the following:

- (1) When did you first prescribe [named medication] for [Worker]?*
- (2) It is my understanding this medication is listed as an [drug category]; has this prescription in [sic.] recommended as [treatment for specified illness] for [Worker]?*
- (3) Was [Worker] on any other [drug in the same category] prior to [Worker's] workplace injury of [date]?*
- (4) What relationship, if any, do you feel this medication has to injury and ongoing [condition]?*

These questions describe a reasonably detailed version of an individual injured worker's medical history. From this fax, it is clear that a named worker had been taking a specific type and strength of medication for an extended period, a few years after suffering an injury at work that may or may not have led to an ongoing condition. That personal information is all compiled in this Privacy Breach, but is noted only by reference in the Privacy Breach Notification.

This was reported and accepted as a minor breach.

When a possible privacy breach is discovered, the WCB's Policy dictates that the manager investigate the breach and classify its severity as either Low (Minor), Medium (Moderate) or High (Major). Every breach discussed above was reported and accepted as a "minor" breach. In addition, in some respects, those classifications do accord with the breach levels as defined in the Policy. As a reminder that definition is as follows:

Low Risk – a breach that affects one or a limited number of people; the information is not inherently of a personal nature (e.g. information that would be found on a business card); the cause has been identified and breach is not ongoing and there is little harm posed to the individual(s) and the organization.

Each of the breaches discussed "affects one or a limited number of people;" in each case, "the cause has been identified and the breach is not ongoing."

However, the question of harm is less clear. There is probably not much information in any of the documents that could be used for extreme financial harm – such as identity theft – but how invasive might the individual find the fact that his/her detailed physiotherapy report was sent to the wrong recipient? The appropriateness of this subjective assessment of harm in classifying the level of the breach will be discussed further below.

All of these breaches also fail the "business card" test that the WCB incorporates into its definition of a "low risk" breach. The breach with the least amount of personal information is the first one discussed, and it includes the worker's name, home address and WCB claim number. I explore this "business card" distinction in greater detail in the next section of this Report.

It should also be noted that the first breach described is the only breach that would meet the example from the Policy of a "low risk" breach. All the others contain significantly more

information than “name, address, claim number,” and seem to more closely mirror the requirements of a “moderate risk” breach, which as a reminder is defined as:

Moderate Risk – a sensitive information breach that affects one or more people; the information is personal (e.g. beyond basic business card information) and unauthorized access to it could place the individual(s) at risk, e.g. identity theft; the cause of the breach may still be unknown; and/or there is a greater risk of harm to the organization.

As these cases show, the definitions of the breach levels are, at times, contradictory, or worse, liable to being cherry-picked. It seems that, ideally, the breach level would be a finding of fact based on specific criteria, by going through a series of “yes or no” questions.

Indeed, the “investigation” stage of the Policy seems to be pointing at making a determination based on a finding of fact:

Investigation will focus on:

- *Scope and cause of the breach*
- *Nature of personal information involved*
- *Degree and risk based on the sensitivity of the personal information*
- *Factors that enhance the impact of the breach*
- *The number of individuals that are affected by the breach*
- *Extent of foreseeable harm to the individual(s) whose information has been breached*
- *Extent of harm to the organization*

I find that the existing breach level definitions are unclear and therefore unable to lead to any consistency or accuracy, insufficient to cover the types of information the WCB handles, and too focused on the potential impact a breach may have on the WCB.

I also find that, even where a breach is discovered that would appear to be at least a moderate breach under the WCB Policy’s rating system, it is often characterized as minor. This may be because the breach ratings are unclear. However, it has the effect of reducing the WCB’s internal responses and responsibilities (i.e. notification).

I find there is some evidence that in the Privacy Breach Notifications, the WCB under-reports the full extent of the personal information disclosed and in doing so may be mischaracterizing a breach as minor when it is in fact moderate or major.

b. Drawing a Distinction in the Definition of Personal Information between “Business-card” Information and “Inherently Personal”

As noted above, the Policy incorrectly labels and classifies personal information and, in particular, it draws a distinction in the information between “inherently personal” or “business-card” information. It is as if the Policy tries to suggest that name, address [usually home address] and WCB claim number of an injured worker is not personal information or is of a lesser category not entitled to privacy protection. However, these pieces of information are very

clearly within the *FOIPOP Act's* definition of personal information, which provides in part as follows:

3(1)(i) "personal information" means recorded information about an identifiable individual, including

(i) the individual's name, address or telephone number,

...

(iv) an identifying number, symbol or other particular assigned to the individual,

Labelling an individual's name, home address and WCB claim number as "business card" information simply serves to muddy the waters. In fact, the inclusion of "WCB claim number" in this list immediately undermines the idea of "business card information." First, the claim number is a unique identifying number assigned to specific individuals and is needed to access government services. Most business cards do not get to that level of detail. It would be analogous to suggesting your health care card number is mere business information.

Second, although a claim number does not necessarily mean a worker is receiving compensation [since the claim can be denied], and the majority of claims to the WCB do represent "no-time-loss" injuries, it does imply parts of an individual's medical and financial history. First, s/he has obviously suffered an injury or illness while on the job. Second, s/he may be receiving compensation to supplement lost wages. It is difficult to imagine any individual choosing to put this information on his/her business card.

Relying on the *FOIPOP Act's* stronger, fact-based definition of "personal information" would help to remove the false suggestion that "business card" information is a separate category of personal information not entitled to privacy protections or entitled to less protection.

Moreover, the "business card" test does not seem to be followed in practice. For instance, in a Privacy Breach Notification dated October 8, 2009, the WCB sent a copy of a worker's physiotherapy progress report to another worker. The progress report contained the first worker's name, date of birth, the WCB claim number, date of injury and some high level details describing the restrictions under which the worker could return to work. However, this level of information was rated as "minor – the offending document contains the name of [worker], [his/her] date of birth and [his/her] WCB claim number. It does not contain [his/her] MSI or Health Card number. The document is a physiotherapy progress report outlining functional capacity for return to work – lifting ability, pain tolerance."

The breach was reported, and accepted as minor. To be clear, physiotherapy progress reports contain personal health information, which is not something that would be found on a business card.

Similarly, in a Privacy Breach Notification dated April 7, 2011, a "Decision Letter" was copied to the wrong employer. Templates for decision letters provided by the WCB on March 24, 2011 included examples of decisions attached to other privacy breach memos and indicated that a good deal of the injured worker's medical and financial history is discussed to provide reasons for a decision.

Even though the wrong employer received a worker's decision, the Manager's risk assessment reads in full: "Low. This breach was reported and accepted as being low."

I find that the WCB has erred in making a distinction in the definition of personal information between business card only and inherently personal. Either information falls within the definition of personal information or it does not. The WCB is not able to divide personal information into classes, one that is entitled to privacy protection and one that is not. The definition of personal information in the *FOIPOP Act* that is referentially incorporated into the Privacy Breach Policy should be adhered to, in full, for all purposes at the WCB.

c. How the WCB Makes a Determinations about the Level of Sensitivity

In addition to creating an artificial split between "business card" and "inherently personal" information, the records reveal that the WCB may be applying a subjective test as the benchmark to determine the level of breach. In a number of Privacy Breach Notifications, those reporting on the breach appear to be weighing the first sentence in the "moderate risk" description. That is, the WCB staff is making determinations about the sensitivity of someone else's personal information to determine the "level" of the breach. The Saskatchewan Privacy Breach Guidelines include in the definition of privacy the following statement:

Information privacy is understood as the right of an individual to determine for him/herself when, how and to what extent he/she will share his/her 'personal information.

A practical example of how privacy is a private matter is found in a Privacy Breach Notification dated October 20, 2009. The WCB sent one worker's Hearing Officer's decision to the wrong worker. The Hearing Officer's decision contained the first worker's name, address and WCB claim number. The opening paragraph of the "Background" section reads as follows:

This worker sustained a fracture of [his/her] [specified body part] on [date], and underwent [specified procedure]. In [year] the Worker was assessed with a [percentage] impairment rating. This was increased to [percentage] in [year]. In [year], the Worker's Compensation Appeal Board considered the worker's appeal for a greater impairment rating. The medical evidence which the Appeal Board had considered at that time was evidence related to the Worker's [specified body part] and [second specified body part] That medical documentation drew a causal connection between the Worker's [specified body part] problem and problems with the [second specified body part] and [third specified body part].

The decision goes on for two full pages discussing the question of whether or not the worker was sufficiently injured to rate a Permanent Medical Impairment, including detailed reasons why or why not.

The risk associated with this document being sent to the wrong worker is assessed as minor because, among other factors, "it does not contain *in [the manager's] opinion*, highly sensitive medical or other information." This Privacy Breach Notification was subsequently accepted "as being low risk . . . and no further action is required".

Again, the Saskatchewan Information and Privacy Commissioner's *F-2007-001* report is instructive:

I do not understand the provision in the procedures of WCB that requires someone to designate whether or not material in any given claim file is or contains "sensitive information". Given the business of WCB, I strongly encourage WCB to view all of its claims files and their contents as "sensitive information" and treat it accordingly. [para. 234].

The WCB should avoid making subjective assessments because where it handles personal health information by definition it should always default to "sensitive." Because of the nature of the WCB's mandate – processing claims of injured workers and planning for their return to work – a large part of the WCB's work involves personal health information: injured workers proving their claim based on information provided by health care providers.

An examination of the definition of personal health information in *PHIA* is also instructive. It provides in part as follows:

"personal health information" means identifying information about an individual, whether living or deceased, and in both recorded and unrecorded forms, if the information

- (i) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,*
- (ii) Relates to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual,*
- (iii) Relates to payments or eligibility for health care in respect of the individual*
- ...*
- (v) is the individual's registration information, including the individual's health-card number,*

As the Saskatchewan Information and Privacy Commissioner wrote in *F-2007-001*:

I start from the position that the personal information and personal health information in the possession of WCB is sensitive and prejudicial. It comprises in very large part either personal health information or personal financial information. It includes detailed diagnostic, treatment and care information from an array of primary providers and specialists. It includes particulars of compensation received from either WCB or through one's employment. [para. 233].

In Saskatchewan, the WCB falls under its personal health information legislation. Different Canadian jurisdictions have taken different approaches to legislating protection of personal health information. For example:

- Newfoundland and Labrador's *Personal Health Information Act* names the Workplace Health, Safety and Compensation Commission, that province's equivalent

of the WCB, as the equivalent of a custodian of personal health information. The *Act* was in effect April 1, 2011.

- New Brunswick's *Personal Health Information Privacy and Access Act* names in the legislation the Workplace Health, Safety and Compensation Commission, that province's equivalent of the WCB, as the equivalent of a custodian of personal health information. The *Act* was assented to on June 19, 2009.
- Ontario's *Personal Health Information Protection Act*, proclaimed in 2004, does not include Ontario's WCB equivalent as a custodian.
- Manitoba's *Personal Health Information Act*, from 1997, does not include that province's WCB equivalent as a custodian.
- Saskatchewan's *Health Information Protection Act*, from 1999, includes all "government institutions" as "trustees" of personal health information. Its WCB falls under this legislation.

Some jurisdictions have legislation that focuses on the *organizations* that hold personal health information, regardless if they are a public body or a private health facility. Other jurisdictions have legislation focused explicitly on expanding the existing public sector privacy provisions to protect *personal health information* itself. The assumption in those cases appears to be that where public bodies possess personal health information, it is well protected by the existing equivalent to the *FOIPOP Act*. Regardless, every jurisdiction that has enacted personal health information legislation has taken the step of saying that personal health information, as a category is so sensitive that governments must take action to protect it wherever it resides.

Nova Scotia's personal health information protections are modeled on Ontario's. The present privacy oversight protections may be sufficient. While the WCB may not fall within the definition of custodian or health care provider under *PHIA*, it is important for the WCB to keep in mind the volume of personal health care information it is responsible to manage and protect.

It is important that the WCB not make its own assumptions on the level of sensitivity of a piece of personal information, because the level of sensitivity of personal information will vary for each individual injured worker. For some individuals the above decision on a permanent medical impairment, with its breakdown of the severity of the injuries suffered, and their possible linkages to each other, may in fact have not been sensitive at all. However, other injured workers may be deeply concerned that someone else is privy to this information without the worker's consent. However, that decision needs to be left to the individual whose personal information is recorded. The WCB should be cognizant that it is the caretaker of all injured workers' personal information including personal health information out of necessity and by law.

Given the mandate and business of the WCB, I find that the WCB should make it clear in its Privacy Policy that staff are to view all claim files and their contents as "sensitive information" and treat it accordingly. I also find that the WCB's Policy and practices should reflect that *privacy is a private matter* and that the impact of the disclosure of personal information should be left for the individual to decide, not the WCB.

d. Major Privacy Breach Characterized as Minor

One incident prior to the adoption of the new Policy is particularly worth noting. On January 8, 2009, the WCB inserted one and two-page letters into an envelope-stuffing machine at the same

time. The result was that 280 letters, 182 of which were addressed and sent to injured workers and 98 of which were copies of worker letters addressed to employers, were stuffed incorrectly in envelopes and therefore at risk of a potential privacy breach. The WCB eventually determined that “there were approximately 71 breaches, with 51 client letters and 20 employer letters not being received by their intended recipients.”

The WCB took action to ensure that the breach was contained and that it knew what information was included in the letters – primarily name, address, some “claim information” and, in some cases, SINs [once again, these breaches demonstrate the weakness of the “business card” test]. The WCB then took the step of attempting to reach every worker and employer potentially affected to notify them of the breach. The WCB provided the Review Office with a copy of the phone script it gave to staff to assist them in contacting those affected by the breach. The records indicate that the WCB achieved “97% compliance” in reaching those potentially affected by the breach by phone, and from that 97% was able to determine that 71 individuals received records to which they were not entitled. The WCB thus created 71 separate “Privacy Breach Notification” memos to document the breach, each of which describes the level of the breach as “minor.”

I find that the WCB’s response to the high volume breach was appropriate in most respects. It tried to contain the problem by contacting the injured workers by telephone. The WCB, however, misconstrued how a high volume breach should be defined. If there is a breach of personal information involving a large number of individuals, even if the amount of personal information in each case is small, it is by the WCB Policy’s own definition a major privacy breach. I find that to have divided this large number into individual minor breaches was not appropriate. This approach does not demonstrate accountability or a commitment to the privacy of injured workers on the part of the WCB. I find the WCB ought to have defined it as a major breach. In private sector businesses, such as banks or retail stores, the public would not tolerate this practice of dividing a large volume breach into multiple minor breaches.

e. Remedial Action through a Direction to Staff

In the WCB’s Privacy Breach Notifications from before the enactment of the Policy and continuing after the formal adoption of the Policy a recurring theme emerges throughout a great many breaches. That is, in 46 out of 155 Privacy Breach Notifications the “remedial action” to prevent future breaches is some version of the statement that “staff were reminded of the importance of verifying that correct information was sent out.” Similar comments were provided as guidance in employee performance appraisal documents for a small number of employees who had a performance goal of zero privacy breaches.

This advice does not seem to be a sufficient solution to the problem, as some staff end up with performance management plans that include a goal of “100% no breaches.”

At most 10 out of approximately 430 employees have performance management goals that dictate they will insure “100% no breaches.” A performance goal structured this way emphasizes protecting the WCB’s confidentiality, rather than ensuring respect for injured workers’ personal information. In addition, the fact that only 10 people have this goal certainly makes it appear punitive involving only those involved previously in a breach, after “reinforcing the importance of double-checking” has failed more than once. This is in contrast to making 100 percent no privacy breaches a professional goal for all employees.

I find that the WCB needs to address the issue of privacy in a much more systematic manner at all levels of the organization through leadership, staff training and clear privacy protection practices. The WCB will, as a result, undergo a cultural shift to a zero tolerance policy: one privacy breach is one breach too many.

f. The Impact of the Recipient on the Level of the Breach

The Policy appears to give undue weight to who the recipient of someone else's personal information is and what that recipient does with the improperly disclosed personal information.

In the breach described under **Inaccurate Classification of Personal Information**, the WCB staff faxed a doctor's office a list of questions that described an injured worker's medical condition in reasonably detailed fashion. The fact that the recipient of the breached information was a doctor, bound by the usual confidentiality expectations of that profession, lends credibility to the "Containment" phase of the breach investigation. In other words, the WCB could take some comfort that the information will not be put to inappropriate uses; it could even help the WCB – when notifying the injured worker as it should have done – to reassure the injured worker that the breach had been contained. However, the nature of the breach – the breach "level" in the Policy – is established by the personal information disclosed. That a doctor received a breach does not mitigate the level of the breach.

An April 22, 2009 Privacy Breach Notification describes a situation in which the WCB staff faxed "some of the worker's medical reports" to the worker's employer in error. This breach was described as minor because "the medical information was sent to an Occupational Health Nurse who is bound by confidentiality."

It was reported and accepted as minor, with no further action required.

Further evidence in the Privacy Breach Notifications suggests that in addition to who received the information, what s/he did with it has been one of the main operating principles on which the WCB determines the severity of the breach.

A Privacy Breach Notification dated December 3, 2009 noted that a worker requested a copy of his/her claim file, which included a Form C for another worker, as well as "physiotherapy reports" for a third worker. The worker who requested his/her file was in the process of filing an appeal of a WCB decision, and had involved an injured workers' association representative to assist him/her in that process. The "Manager's Risk Assessment" is as follows:

I assess the risk of this breach to be High [although the check box in the header was marked "Moderate"]. There have been two separate documents added to the incorrect claim file involving two workers other than the appropriate injured worker. The injured worker has involved [Injured Workers' Association] to help [him/her] through the claims process and [Injured Workers' Association representative's name] has become aware that a breach of confidentiality has occurred. At this point in time, the information contained in the specialist's report for [third injured worker] would be, on its own, considered a moderate breach as there was personal information contained within the report. The Physiotherapy Report for [second injured worker] is considered a minor breach.

The reference to the Injured Workers' Association is entirely linked to the impact the disclosure of personal information has on the WCB as an organization; it is irrelevant to the severity of the breach. In this case, one of the workers whose personal information was sent to the first injured worker was notified by letter; the other was not.

The breach was reported and accepted as moderate, with no further action required.

Two significant privacy breaches within about one month of each other also point to the fact that the WCB is emphasizing its own interests ahead of the individual injured worker whose privacy has been breached.

The first is in a Privacy Breach Notification dated December 10, 2010. The notification indicates an injured worker requested a copy of his/her file. The WCB printed off the complete file of a second injured worker, and sent the complete file to the worker who requested his/her own file. The first worker, who received the complete file of the second in error, called the WCB, which sent a courier to recover the second worker's file from the first worker. The breach was described as minor:

[The worker receiving the file] acted in a responsible manner by keeping the materials secure, immediately contacting us and arranging to have all the materials promptly returned to us.

This breach was reported and accepted as minor, and no further action was required. The second worker was never told that his/her complete file was disclosed to a third party.

Just over one month later, on January 13, 2011, a Privacy Breach Notification was submitted which describes the identical situation: a worker requested his/her file, and received a complete copy of another injured worker's file instead. In the header of this Privacy Breach Notification, the Manager's Risk Assessment was checked off as "Other," with a footnote indicating "pending further information." In this case, the WCB was unsure of what the recipient had done with the other injured worker's records, but it believed s/he may have made private arrangements to deliver the records to the other injured worker whose personal information had been disclosed. In addition, the WCB believed that the recipient may have been in contact with the media.

The risk assessment on this breach was as follows:

Moderate at this time – we have been unable to speak with [the worker who received the records] to date to validate our information that the materials that do not belong to [him/her] have been handled in a confidential manner and returned to [the other injured worker]. Phone calls on January 12 and January 13 have not been returned. Letters will be sent in order to communicate with parties involved.

In this case, both workers received communications from the WCB notifying them of the breach and indicating the WCB would be reviewing its processes and apologizing for the error.

The WCB did not provide the Review Office with documentation indicating that an internal response to this Privacy Breach Notification was provided, so it is unclear whether any additional feedback was ever provided.

I find that the WCB uses inappropriate factors in measuring the level of breach and its response to the breach: who receives the disclosed personal information, what the recipient does with the personal information received, and, most importantly, what the impact of the breach is on the WCB. The WCB needs to apply its own definition of privacy breach consistently and to proactively ensure notification and containment. These issues will be discussed below.

g. Whose Risk is Being Assessed?

Part and parcel with the emphasis on what the recipient does with the record is the WCB's emphasis on its own exposure to risk in assessing a breach. It is certainly important to consider the risk to which an individual is exposed as a result of his/her privacy being breached. The Policy, however, incorporates both risk to the individual and the organization, in other words, the WCB itself, into the definitions of the breach levels.

The first test needs to be about the type of personal information and then the quantity of information disclosed. The Policy, by including all the tests in the same sentence, lacks clarity. As a result, the risk level is sometimes the entire measure by which a breach level gets determined, as when a request for a worker's medical information was sent to the wrong doctor on February 10, 2010. The risk in this case was described as "minor" because the breach "is contained, the cause has been identified, it is not ongoing, the[re] was no medical information sent, and it was another service provider so minimal risk is posed to the individual."

While this may, indeed, have been a minor breach based on the limited amount of an injured worker's personal information actually disclosed, it is troubling that an examination of that personal information is almost entirely absent from this risk assessment.

Similarly, the breaches discussed above in the section on who was the recipient of the breach highlight the WCB's emphasis on the risk to itself, rather than the nature of the breach or the risk to the injured workers. We have evidence of two privacy breaches that are identical in every respect except that one of the recipients planned to go to the media, while one of the recipients simply sent the file back to the WCB. Where it loses control of what the recipient does with the disclosed information, the WCB finds itself at greater risk, and so adjusts the classification of the privacy breach.

I find that the WCB places an undue emphasis on risk to itself as an organization in making a determination as to the level of the breach. Risk factors such as the risk of liability to the WCB if disclosure of personal information results in identity theft or risk of embarrassment if a privacy breach becomes a matter of media interest will inevitably be considerations for the WCB. I find, however, that the WCB needs to change its focus under the Policy to make the privacy interests of the injured workers paramount and central.

h. Failure to Provide Notification to Injured Workers

Under the Privacy Breach Policy, the WCB has the discretion on whether or not to notify those affected by moderate to high-level breaches. The Policy reads as follows:

- *In cases of moderate to high level breaches, it may be appropriate to contact the individual(s) whose personal information was the subject of the privacy breach depending on the outcome of the investigation*
- *Individuals should be informed of a privacy breach and the specific information disclosed when there is a significant risk of:*
 - a) *Harm or embarrassment to the individual or company*
 - b) *Public disclosure of the personal or corporate information*
 - c) *Opportunity for malicious use of the personal or corporate information*

The Policy is silent on notification for minor or low risk breaches.

From the records and evidence provided by the WCB, it appears that one portion of this test is primarily used: individual injured workers affected by a breach seem to be notified when there is a risk of embarrassment to the WCB because the affected individual already knows or will likely come to know about the breach.

As discussed above, on January 8, 2009, the WCB had a malfunction in its mailroom, leading to a single incident that the WCB describes as 71 unique, “minor,” breaches. All the injured workers involved were contacted by phone to notify them of the potential breach. This was a case where there was a strong possibility of injured workers receiving a portion of a letter that was not intended for them, and so discovering there was a disclosure issue.

Of the remaining 84 Privacy Breach Notifications, those injured workers whose personal information was disclosed were notified 11 times. Seven of those notifications occurred in “Minor” breaches, three occurred in “Moderate” breaches, and one occurred in a breach that was labeled moderate, but downgraded to “Minor” after a Legal Services review.

In a July 17, 2009 Privacy Breach Notification, an injured worker received the written decision of another injured worker, called to notify the WCB, and indicated that s/he would be keeping the record in a sealed envelope with his/her lawyer. The same worker received the same decision in error a second time, when the WCB tried to mail out the decision to the correct worker. The injured worker whose decision was mailed out to the wrong injured worker was notified in this case by phone.

A Privacy Breach Notification memo dated December 3, 2009 indicates that Worker A received a copy of his/her claim file. Within the file was a physiotherapy report on Worker B, so Worker A contacted and advised the WCB of this. The WCB created a Privacy Breach Notification dated October 8, 2009, labeling the breach minor. Worker B was never contacted. Later, Worker A realized that his/her file also contained a doctor’s examination of Worker C. The WCB notified Worker C that his/her information was contained in another worker’s file. The first contact was by phone and then subsequently by letter, sending a copy of the misfiled document to Worker C for his/her review. The records were returned to the WCB and this breach appears to have been contained.

In a Privacy Breach Notification dated January 5, 2010, Summary Decisions and Reports and envelopes were printed for two separate injured workers. However, those decisions were placed in the wrong envelopes and mailed out. When the first injured worker received someone else’s decision, s/he called the WCB to report it, and advised s/he would destroy the record. The WCB

then contacted the second worker affected by the breach, and ask that s/he destroy the incorrect record as well.

A December 15, 2010 Privacy Breach Notification indicates that an injured worker received a letter about another worker, and that the WCB had the incorrect address. On reviewing the records, the WCB discovered that the form provided by the doctor who examined the worker included the worker's incorrect address. The WCB therefore called the worker to notify him/her of the breach and update his/her address. Effectively the same situation was noted in a Privacy Breach Notification dated January 5, 2010, which was a different memo from the January 5, 2010 Privacy Breach Notification discussed above.

The breach reported on January 13, 2011 has been discussed at length above. In that situation, the injured worker who had received the other worker's information incorrectly had made contact on his/her own initiative with the affected injured worker, and the WCB contacted both parties to discuss the situation.

On January 20, 2009, a Privacy Breach Notification indicated that an individual who had been representing a worker had asked for and received the worker's file. The worker, however, no longer wished to be represented by the representative. S/he therefore called the WCB when s/he found out the former representative received his/her file. In this case, the worker was notified of the breach, the WCB discussed it with him/her and apologized, but notification was more on the worker's initiative than the WCB's.

A Privacy Breach Notification dated December 20, 2010, indicated that a request for a physician's report on one worker was sent to the physician, and copied to the worker. However, the request had a second worker's name, WCB claim number, health card number and date of birth in the "Re:" line. Both the first and second workers were contacted to discuss the issue, and the first worker indicated s/he would destroy the letter.

A similar example was reported in a Privacy Breach Notification dated February 2, 2010. The wrong worker received notice of a new injury, and the importance of reporting the injury to the WCB in a timely fashion. The recipient called and advised the WCB that s/he had received the letter in error and would destroy it. The WCB followed up by contacting the injured worker whose privacy had been breached to notify him/her.

One non-privacy breach incident was recorded on a Privacy Breach Notification by the WCB, though it did well to identify the situation as a potential concern and stop it early. A Worker's Representative faxed a notice of appeal, including all supporting documents to the WCB for one worker. The last two pages of the 62-page submission were related to another worker. The WCB deleted the last two pages, and contacted both the Worker's Representative and the second worker to notify them of the mix-up. It does not appear that the WCB contacted the first worker.

The final Privacy Breach Notification that indicated notification was attempted was recorded on April 7, 2011. In this circumstance, a decision letter was sent to the worker, but carbon-copied to the wrong employer. The worker's version of the letter named the wrong employer in the "cc" line. The WCB contacted the worker to notify him/her of the breach, and to provide a copy with the correct employer listed.

In short, of the 11 notifications, four were circumstances in which the worker affected by the breach already knew or was likely to learn of the breach, two involved an incorrect address, and one was not a breach by the WCB. The remaining four were situations where the WCB can be said to have given notice to an injured worker who was not already aware of a breach, solely for the purpose of notifying the injured worker that a breach had occurred.

More troubling is the fact that there are, throughout the records, many examples of similar breaches with the affected worker not being notified. It is difficult to conceive of an explanation for this difference in approach. It certainly suggests that the protection of individuals' personal, private information is not a given priority emphasis over protecting the WCB from the embarrassment a breach might cause.

I find that the WCB rarely notifies individuals when their privacy may have been breached. Excluding the single incident characterized as 71 unique breaches, notifications have only been sent 13% of the time. This also demonstrates the WCB's tendency to minimize the impact any particular breach may have on an individual injured worker.

I find that the Policy appears to encourage the lack of notification by making it discretionary in all cases, focusing the impact of the breach on the WCB as an institution and allowing for a broad range of disclosures to be categorized as "minor."

i. Changing the Determination of the Breach Level

Of the 155 unique privacy breaches, managers reported Privacy Breach Notifications indicating a "Moderate" breach in 11 instances. In its response to the Privacy Breach Notifications, the Legal Services Privacy Breach Coordinator downgraded seven of those "moderate" breaches to "minor," and upgraded three "minor" breaches to "moderate."

The Investigation stage of the Policy assigns "the manager responsible of the area where the breach occurred" with responsibility to "lead the process to investigate and document the cause of the breach." As discussed above, the initial investigation into a privacy breach needs to be a finding of fact, and on that basis there should not be any discretion in the Policy to modify a breach classification after the manager investigating files his/her report, unless detailed evidence shows an error in the fact-finding.

Legal Services policy-directed role in "Management of the Breach" is to "track the status of the breach and provide a memo to the manager with any feedback from legal services."

Modifying the "level of breach" findings of a Privacy Breach Notification would seem to come back to some lack of clarity on the part of the Policy in defining the nature and scope of the breaches.

The record disclosed in the January 21, 2011 breach that was labeled "Minor." The response from the Legal Services Privacy Breach Coordinator to the Manager stated:

Based on the details you provided and the personal information involved, I would assess the risk as moderate and ask that you amend your record to reflect this. No further action is required.

In the Legal Services Privacy Breach Coordinator's response to the Manager regarding a January 26, 2011 breach labeled minor, she stated:

Based on the details provided, I would assess this privacy breach as moderate. [The worker affected by the breach] was not advised of the breach, the correspondence sent in error has not be returned to the WCB (to our knowledge) and the information contained on the document involved falls within the definition of a moderate risk breach: [quotes definition].

Almost the exact same wording was used in response to a February 4, 2011 breach. If the WCB is indeed changing its privacy practices to ensure that the worker affected by a breach is always notified of the breach, I would find that commendable. However, given the WCB's past practices with respect to notification, it seems capricious to change breach levels on that basis now. Moreover, though notification of those affected by a breach is a best practice, it does not in fact alter the level of severity of a privacy breach.

The reverse situation is troubling as well. On February 25, 2011 and again on April 14, 2011, managers reported breaches they described as "Moderate." The response from the Legal Service Privacy Breach Coordinator to the Manager was as follows:

I accept the risk assessment of the breach as being low; and based on the details provided and [sic] no further action is required.

No other information is contained in the records to explain this change.

I find there to be inconsistencies in how the definitions of the privacy breach levels are applied by the WCB. I also find the documentation provided back to managers lacks substantive helpful advice or guidance particularly where the breach level has been changed. There is no discretion in the Policy to change the classification of a breach without detailed evidence showing facts are wrong.

j. The Role of the Privacy Breach Advisory Committee

The last stage of a privacy investigation, under the WCB's Policy, is Follow-up and Prevention of Future Breaches. One of the ways that the Policy envisions this follow-up and prevention is through the Privacy Breach Advisory Committee. Under Step five of the Policy, this Committee is given the following directive:

In the case of moderate and high risk breaches, the Privacy Breach Advisory Committee will provide a separate quarterly report debriefing the incident for the Executive Team and the organization – intent is to capture the "learnings" and recommend future preventative actions.

Since the WCB has begun tracking privacy breaches, it has not reported a single "high-risk" breach, and of the 155 breaches it has reported, seven have been reported as "moderate." Six of those moderate breaches have occurred after the adoption of the Policy. However, the WCB confirms, in a response to questions from the Review Office dated May 20, 2011, that the Privacy Breach Advisory Committee has produced no documentation as of that date.

I find the Policy requires a committee that is populated by all the major business areas of the WCB and that this model is ideal for addressing follow-up and prevention of privacy breaches because it provides for a systemic approach. Unfortunately, I also find that there is no evidence that a Privacy Breach Advisory Committee has ever been established and properly constituted in accordance with the Policy and, therefore, I find that the WCB is in breach of its own Policy by failing to do so. Further, I find that the principal means by which the WCB and its executive can receive assessment and advice regarding privacy breaches within the organization is unfortunately completely missing. The Privacy Breach Advisory Committee should have been properly constituted to do the work as contemplated by the WCB's Policy.

10. Findings:

1. Section 27 of the *FOIPOP Act* does not authorize the WCB to release one injured worker's personal information to another injured worker. I find the disclosure of the personal information constitutes a breach under the *FOIPOP Act*. I find that the WCB acknowledges it had no authority to disclose the personal information in the manner that is subject to this Review. While there was no evidence the releases were intentional, malicious, or purposeful, the breaches remain serious.
2. I find that the collection, retention, use and disclosure of personal information makes up a large part of the "industry" of the WCB.
3. I find that the WCB has fallen short under its own Privacy Breach Policy. While the promoting accountability and monitoring compliance provisions of the Policy are mostly adequate, they are not followed. The WCB has failed to follow its own Policy as follows:
 - a. The designated manager has not reported to the Privacy Breach Advisory Committee as the WCB has failed to constitute the Committee;
 - b. The designated manager is accountable to promote and implement the Policy but has fallen short to ensure it is fully implemented and followed;
 - c. Legal Services is required by the Policy to provide statistics on privacy breaches to corporate but this does not appear to have been done.
4. I find that the existing breach level definitions are unclear and therefore unable to lead to any consistency or accuracy, insufficient to cover the types of information the WCB handles, and too focused on the potential impact a breach may have on the WCB.
5. I also find that, even where a breach is discovered that would appear to be at least a moderate breach under the WCB Policy's rating system, it is often characterized as minor. This may be because the breach ratings are unclear. However, it has the effect of reducing the WCB's internal responses and responsibilities (i.e. notification).
6. I find there is some evidence that in the Privacy Breach Notifications, the WCB under-reports the full extent of the personal information disclosed and in doing so may be mischaracterizing a breach as minor when it is in fact moderate or major.
7. I find that the WCB has erred in making a distinction in the definition of personal information between business card only and inherently personal. Either information falls within the definition of personal information or it does not. The WCB is not able to divide personal information into classes, one that is entitled to privacy protection and one that is not.

8. Given the mandate and business of the WCB, I find the WCB should make it clear in its Privacy Policy that staff are to view all claim files and their contents as “sensitive information” and treat it accordingly. I also find that the WCB’s policies and practices should reflect that *privacy is a private matter* and that the impact of the disclosure of personal information should be left for the individual to decide not the WCB.
9. I find that the WCB’s response to the high volume breach was appropriate in most respects. It tried to contain the problem by contacting the injured workers by telephone. The WCB, however, misconstrued how a high volume breach should be defined. If there is a breach of personal information involving a large number of individuals, even if the amount of personal information in each case is small, it is by the WCB Policy’s own definition a major privacy breach. I find that to have divided this large number into individual minor breaches was not appropriate. This approach does not demonstrate accountability or a commitment to the privacy of injured workers on the part of the WCB. I find the WCB ought to have defined it as a major breach. In private sector businesses, such as banks or retail stores, the public would not tolerate this practice of dividing a large volume breach into multiple minor breaches.
10. I find that the WCB needs to address the issue of privacy in a much more systematic manner at all levels of the organization through leadership, staff training, and clear privacy protection practices. The WCB will, as a result undergo a cultural shift to a zero tolerance policy: one privacy breach is one breach too many.
11. I find that the WCB uses inappropriate factors in measuring the level of breach and its response to the breach: who receives the disclosed personal information, what the recipient does with the personal information received, and most importantly, what the impact of the breach is on the WCB.
12. I find that the WCB places an undue emphasis on risk to itself as an organization in making a determination as to the level of the breach. Risk factors such as the risk of liability to the WCB if disclosure of personal information results in identity theft or risk of embarrassment if a privacy breach becomes a matter of media interest will inevitably be considerations for the WCB. I find, however, the WCB needs to change its focus under the Policy to make the privacy interests of the injured workers paramount.
13. I find that the WCB rarely notifies individuals when their privacy may have been breached. Excluding the single incident characterized as 71 unique breaches, notifications have been sent only 13% of the time. This also demonstrates the WCB’s tendency to minimize the impact any particular breach may have on an individual injured worker.
14. I find that the Policy appears to encourage the lack of notification by making it discretionary in all cases, focusing the impact of the breach on the WCB as an institution and allowing for a broad range of disclosures to be categorized as “minor.”
15. I find there to be inconsistencies in how the definitions of the privacy breach levels are applied by the WCB. I also find the documentation provided back to managers lacks substantive helpful advice or guidance particularly where the breach level has been changed. There is no discretion in the Policy to change the classification of a breach without detailed evidence showing facts are wrong.
16. I find the Policy requires a committee that is populated by all the major business areas of the WCB and that this model is ideal for addressing follow-up and prevention of privacy breaches because it provides for a systemic approach. Unfortunately, I also find that there is no evidence that a Privacy Breach Advisory Committee has ever been established and properly constituted in accordance with the Policy and, therefore, I find that the

WCB is in breach of its own Policy by failing to do so. Further, I find that the principal means by which the WCB and its executive can receive assessment and advice regarding privacy breaches within the organization is unfortunately completely missing. The Privacy Breach Advisory Committee should have been properly constituted to do the work as contemplated by the WCB's Policy.

11. Recommendations

- 1) The WCB's Annual Report speaks of changing leadership cultures to ensure safe work practices. It notes that "Our community needs to embrace a very simple ideal – that one Nova Scotian injured on the job is too many." This is a laudable goal. The Privacy Review Officer, however, recommends that the WCB take that same view of ensuring best privacy practices at the WCB: best privacy policies and practices will only come with an effort to make privacy a top priority and when the WCB accepts that one privacy breach is too many.
- 2) The WCB is highly cognizant of the self-worth component of working: i.e. dignity, autonomy, making meaningful contribution (as an example, see the "Rod Stickman" videos at www.worksafeforlife.ca). The WCB's emphasis on the importance of these values is commendable. Privacy, however, is as important in achieving these values, and in helping workers back to work, or assisting those who can never go back, the WCB needs to be cognizant of the self-value of privacy. Workers have to give up their personal privacy – i.e. a fundamental part of themselves, their dignity and their ability to be autonomous – to the WCB in the course of pursuing a claim and return to work. The Privacy Review Officer, however, recommends that the WCB needs to put privacy on a higher plane and recognize that it is the guardian of sensitive personal and personal health information.
- 3) I strongly recommend that the Privacy Breach Advisory Committee as described in the Privacy Breach Policy be constituted, and that it should meet on at least a quarterly basis to examine all Privacy Breach Reports. The Committee should proceed with its policy-dictated function of producing a quarterly report to "document the learnings" from any breaches and should be available to meet when more urgent breaches arise. The Committee could also be responsible for contributing to and monitoring the effectiveness of any revised breach definitions in the Policy coming out of this Privacy Review.
- 4) I recommend that the Privacy Breach Advisory Committee become an internal promoter of best privacy practices. The Committee could do so through its quarterly reports that could be circulated through an employee newsletter.
- 5) I recommend the Privacy Policy remove any reference to discretion in determining the level of breach. The determination of the breach level must be a finding of fact and needs to be investigated as such.
- 6) I recommend the breach classifications need to be re-written for greater clarity, and the classifications need to be based on (in priority order): (1) the kind of personal information; (2) the volume of personal information; (3) to whom the personal information was improperly disclosed and the extent of the breach; (4) the potential harm to the affected individual(s) as a result of the breach. An example follows:
 - To be categorized as minor, you must be able to answer *yes to all* of the following questions:

- Was the information disclosed limited to the injured worker's name, address, phone number and employer's name?
 - Was the release of the personal information contained to only a small number of injured workers (3 or fewer)?
 - Has the personal information been recovered?
 - Is the cause of the privacy breach known, and has it been contained?
- A minor breach ***must also include a no*** to the following questions:
 - Did the information contain details of the worker's injury and/or his/her requirements for a successful return to work?
 - Did the information contain the injured worker's Social Insurance Number [SIN], Health Care Number, WCB claim number and/or date of birth?
 - Has the same type of breach occurred within the same unit at the WCB within the last three months?
 - Is there enough identifying personal information in the disclosure to re-create the individual's detailed contact information that could be used for identity theft?
- If you answer ***yes to any*** of the following questions, the breach would be considered ***at least moderate***:
 - Did the disclosed information contain the injured worker's date of birth or SIN?
 - Did the disclosed information contain high-level details of a worker's injury or return to work needs and was it sent to someone other than the worker's employer?
 - Was more than one individual's information disclosed at once?
 - Did more than three but fewer than 10 individuals receive the information?
 - Is the cause of the breach unknown, and therefore the breach has not been contained?
 - Does the information disclosed meet the standards of a major breach, but it has been disclosed to a WCB third party service provider, who is also bound by WCB's Privacy Policy? How has the WCB satisfied itself that the WCB third party service provider complies with the WCB's Privacy Policy?
 - Has the same type of privacy breach occurred within the last three months?
- If you answer ***yes to any of the following questions***, the breach would be considered major:
 - Does the disclosed information contain the detailed health care history or doctor's charts of an injured worker, including such disclosure to the worker's employer?
 - Does the disclosed information relate to, or was it sent to 10 or more individuals?

- Is the breach the result of an external attack? This relates more to information technology and security than it relates strictly to privacy, but the problem with the existing Privacy Breach Policy is that it appears to be more a security-based policy than privacy-based. The difference being that security relates to how the WCB manages the information, whereas privacy relates to the individual injured workers.

- 7) I recommend that the WCB apply its own definition of privacy breach consistently and to proactively ensure notification to injured workers and containment of the breach.
- 8) I recommend the WCB look for ways to scale back the amount of personal information that it discloses during its day-to-day operations. The WCB's objective to get the injured worker back to work safely and healthy is very important. To do this, it seems employers would need a fairly limited amount of information: what did the employee injure, how did s/he injure it and what medically approved steps need to be taken to ensure a healthy and successful return to work? Limiting the disclosure to what is specifically needed for that purpose is consistent with the *FOIPOP Act*, and it will help to mitigate against a potentially larger breach if the information is sent to an incorrect location. In part it will do so by requiring the individual WCB employee responding to the request for disclosure to turn his or her attention to the file, what needs to be included in the disclosure, to whom it is being sent and how.
- 9) Where it is determined that employee performance plans should include a goal for maintaining privacy, the focus should be on ensuring that the privacy and dignity of injured workers is protected not on disciplining employees or protecting the WCB. I recommend including a commitment to protection of privacy as part of all employee performance plans and note that the emphasis should not be on privacy breaches, which comes across as punitive. The goal could, however, be measured by ensuring that the worker who breached the personal information made a vigorous effort to recover and contain the breach, and made every effort to notify the individual whose privacy may have been breached within a reasonable timeframe thus demonstrating a commitment to the importance of protecting privacy.
- 10) I recommend that notification of the individual whose privacy may have been breached should be done in all cases, regardless of the level of the breach. To reconfigure the attention the WCB pays to privacy requires that each and every example of the disclosure of personal information is addressed with the affected individual.
- 11) I recommend that individuals be notified when their privacy *may* have been breached. One of the WCB's core values is to be "Caring and Compassionate," which it explains in its Annual Report as "striv[ing] to walk a mile in workers' and employers' shoes. We will serve as we like to be served and provide those we serve with the respect and support they need to be successful." It would seem that part of this would be not to allow employees to make assumptions about whether or not a privacy breach would be a concern for a particular injured worker.
- 12) When notifying individuals of a privacy breach, I recommend that the WCB make clear that workers have the right to file a privacy complaint with the WCB, that will be separate and distinct from their WCB claim file; and that if the worker is unsatisfied with the WCB's response, s/he has the right to file a Request for Review with the Review Officer. The WCB should create and demonstrate a protective screen to ease injured workers' concerns in this regard.

- 13) The WCB has not produced a privacy complaint policy to date. I recommend that the WCB develop a privacy complaint policy that is publicly available, on its website and includes how complaints will be processed to guard against retribution.
- 14) The public body sending information bears the responsibility to ensure that the personal information it is sending is accurate. I recommend that the WCB should, therefore, modify the 8/10 form, on which doctors report on injured workers' visits, to ensure that form is updated every time the injured worker sees the doctor (for instance, perhaps by adding a check box on the form that confirms the doctor has verified the patient's employer), and/or the WCB should confirm with the worker that it has the correct employer before sending information off to what the WCB believes is the correct employer.
- 15) I recommend that the WCB ensure that it recovers *all* personal information it has inadvertently disclosed and it should not be attempting to pass on any costs of doing so. It is not sufficient to rely on the incorrect recipient injured worker or health care provider to destroy the information received. I further recommend that the WCB bear all costs associated with having the personal information returned to or retrieved by its offices.
- 16) The WCB appears to be moving away from identifying individuals solely by their WCB claim number, and I recommend this practice continue. Relying on multiple identifiers will assist the WCB to guard against misdirecting personal information to the wrong person.
- 17) If practical, I recommend that an injured worker's CW should act as a second pair of eyes on a file containing personal information before it is mailed out.
- 18) I recommend that the WCB make its Privacy Policy readily accessible on its website and make it patently clear on its website that all approved service providers will be bound by the WCB Privacy Policy.
- 19) I recommend that the WCB incorporate the *FOIPOP Act's* definition of personal information directly into the Privacy Breach Policy (and not just referentially incorporate it), and make note, as a best practice, that the WCB also collects and uses the sensitive personal health information of injured workers.
- 20) Organizations do not have privacy rights and thus I recommend that the Policy should not include the risk of harm to an organization as part of the metric for determining the severity of the breach.
- 21) I recommend that the WCB amend its Policy to require notification of the injured worker whenever a privacy breach occurs, and regardless of the classification of the breach level.

Subsection 5(1)(a) of the *PRO Act* states:

5 (1) In addition to the Privacy Review Officer's duties and powers referred to in Section 6 with respect to reviews, the Privacy Review Officer may

(a) monitor how the privacy provisions are administered and conduct reviews of privacy complaints arising from the privacy provisions; . . .

Pursuant to s. 5(1)(a) of the *PRO Act*, the Review Officer will be monitoring the WCB on its progress implementing these recommendations by requiring the WCB to provide updates within the next year at three month intervals.

12. The WCB's Response to the Recommendations

Prior to making this report public, I chose to share a draft of the Report with the WCB in order to confirm that the Review Office's understanding of the facts supporting my findings and recommendations was correct, and to ascertain how many recommendations WCB would be prepared to accept. That draft was shared on October 25, 2011 and the WCB's response was received at the Review Office on November 9, 2011.

With regard to the acceptance of recommendations, the WCB responded as follows:

Accept and will implement immediately: 1, 2, 3, 4, 13, 15, 16

Accept in principle, but need time to implement: 5, 6, 7, 8, 9, 10, 11, 12, 14, 17, 18, 19, 20, 21

The WCB's response also included the following comments on the Privacy Breach Advisory Committee:

Although the committee has recently been formally struck, and it is in its infancy, it has met.

It was only when the WCB responded to the draft Report that the Review Office learned that the Privacy Breach Advisory Committee had been constituted and had in fact met. Completion of the recommendations regarding the Committee will be reviewed as part of the ongoing monitoring.

As stated above, this Report requires the WCB to provide progress reports on its implementation of the recommendations over the course of the next year.

Respectfully,

Dulcie McCallum
Freedom of Information and Protection of Privacy Review Officer