SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2012-005

Saskatchewan Government Insurance

Summary: The Office of the Information and Privacy Commissioner (OIPC) received a formal 'breach of privacy' complaint that related to the "use" by Saskatchewan Government Insurance (SGI) of personal information and personal health information of a claimant (hereinafter referred to as the Complainant) under *The Automobile Accident Insurance Act* (AAIA). The Complainant alleged that too many employees at SGI had access to her personal information and personal health information. The Complainant was an employee of SGI and had filed an injury claim following a motor vehicle accident. SGI took the position that the OIPC had no authority to investigate these matters since neither *The Health Information Protection Act* (HIPA) Parts II, IV and V, nor *The Freedom of Information and Protection of Privacy Act* (FOIP) applied to the Complainant's personal information and personal health information as it related to Part VIII of AAIA. The Commissioner considered representations from SGI and, consistent with past Reports issued by the Commissioner, concluded that there is no evidence that the Legislative Assembly would have intended to create such a gap in legislated privacy protection and that, in fact, there is no such gap as alleged by SGI. The Commissioner, however, recommended that the Legislative Assembly amend the appropriate legislation to clarify the rules that will apply to the personal information collected, used and disclosed by SGI in its activities under the AAIA and the role of the OIPC in overseeing SGI's statutory responsibilities under FOIP and HIPA. He also recommended that SGI provide an apology to the Complainant and enhance its user access policies and procedures.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, ss. 2(1)(d)(ii), 23, 24 and 28; *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1, s. 12; *The Health*

Information Protection Act, S.S. 1999, c. H-0.021, ss. 2(m), 2(t)(i), 4, 16, 23 and 26(3); *The Automobile Accident Insurance Act*, S.S. 1978, c. A-35.

Authorities Cited: Saskatchewan OIPC Review Reports F-2007-002, F-2007-001, F-2006-005, LA-2010-002, LA-2010-001, LA-2007-002, Saskatchewan OIPC Investigation Reports F-2012-001, F-2010-001, F-2009-001, F-2007-001, H-2011-001, H-2004-001.

Other Sources Cited: Saskatchewan OIPC, *Report on The Health Information Protection Amendment Regulations, 2010*, *Glossary of Common Terms: The Health Information Protection Act, 2010-2011 Annual Report*, *A Contractor's Guide to Access and Privacy in Saskatchewan*; Canadian Human Rights Commission, *A Guide For Managing The Return to Work*; ISO Standards, *Information Technology – Security Techniques – Code of practice for information security management*, International Standard ISO/IEC 17799; Province of Saskatchewan, *An Overarching Personal Information Privacy Framework for Executive Government;* WorkSafe Saskatchewan, *Fact Sheet: WCB Standard RTW Definitions (Section 1.4)*.

I BACKGROUND

[1] The Complainant contacted our office on May 26, 2009 requesting an investigation into an alleged breach of her informational privacy by Saskatchewan Government Insurance (SGI).

[2] The Complainant was an employee of SGI and had been involved in a motor vehicle accident which resulted in her filing an injury claim with SGI. The Complainant's concerns involved the handling of her injury claim as an employee by SGI.

[3] The salient issues were stated by the Complainant in her letter to our office dated May 23, 2009:

> The total number of SGI employees that I am "aware" of to date (in and out of scope) who have had access to the on-line portion of my injury file is eighteen plus at least two in the Income Benefit Calculation Unit.
> …

> [T]here have been four occasions that I am "aware" of, during my claim, when confidential information has been directed to the Regina Injury Claims Centre and opened by clerical staff, despite the fact that I have been advised my claim is being handled with confidentiality outside of my office.
> …
>
> I do not understand why the SGI Head Office managers for [Saskatchewan] Injury North and Injury South and the Assistant Vice President of Claims all require access to my claim. If there is a problem on the claim that requires their input, should they not be required to apply for access at that time and have a valid reason for doing so? Or why is the claim initiated in my own department and access to it given to my manager, my supervisor and three senior Personal Injury Representatives? Is there a legitimate business need for each of them to have access to my file? Or why do a similar group of employees in Saskatoon "all" require access to my file? And why, when my claim was transferred from Regina to Saskatoon, were the manager and supervisor in my office allowed access to my claim, just by sending an email to Claims Administration Department in Head Office and requesting it? Did they have a legitimate business reasons for the request? And why would they require access to my auto as well as my injury claim?
>
> I do not feel that access to my file should automatically be granted to a list of SGI employees who I know and work with.

[4] The Complainant's letter also stated:

> It is very uncomfortable to meet with people in a work capacity, who know your most intimate medical information as well as intimate personal history (as compiled by assessment teams).
> …
>
> Prior to my motor vehicle accident all my performance reviews were positive and since my claim, my work situation has deteriorated and this is very distressing to me.

[5] On June 12, 2009 the Complainant provided further information. Included in the submission was the following:

> Please note that from February 5, 2007 to February 13, 2007 all Personal Injury Representatives in all Injury Centres in the province would have had been able to access my online claim.

[6] On September 4, 2009 I met with the Chief Privacy and Ethics Officer and Assistant Vice President of Injury Claims and Rehabilitation for SGI as part of my office's investigation.

[7] On October 15, 2009 my office received a submission from SGI which stated the following:

> All staff claims are handled by an office other than the office in which the staff person is employed. As regards injury and general claims, these are assigned to independent adjusting firms.
>
> As you can appreciate, the primary concern in the handling of staff claims and their families is to ensure that employees claims are adjusted fairly, that SGI's Corporate image is protected and that no undue pressure is placed on adjusting staff attending to these claims.
>
> The SGI "Staff Claims Procedures (Auto) [sic] states:
>
> > SGI branch employee's or their immediate family members claims must be reported to and handled by a claims center other than the one in which the employee works…the damage appraisal must be reviewed and approved by the Manager of Appraisals South or North as applicable and the file noted accordingly.
> >
> > Before payment is made on any employee claim or that of an immediate family member, the Branch Manager must review and approve payment. Claims involving management must be reviewed and approved at the next higher level of authority…
> >
> > …the Branch Manager for the branch handling the claim should also arrange for restricted access to only those persons at the branch handling the claim who have a business need to access the file along with the Head office Manager.
>
> [The Complainant's] injury file was assigned to [independent adjuster] of [private company]. Unfortunately, the injury program available under *The Automobile Accident Insurance Act* is complex and requires a level of expertise that most independent adjuster [sic] simply have not acquired. Accordingly, despite the fact an independent adjuster is handling the file, the claim is overseen by SGI Claims staff. In [the Complainant's] case, Saskatoon Injury took over Management of her file. [Saskatoon Personal Injury Representative] was the adjuster assigned to monitor the progress of the independent adjuster.

[8] Based on the material provided by both SGI and the Complainant, it appeared that approximately 43 separate individuals may have had access to the Complainant's injury claim information for different reasons at different times.

[9] On June 12, 2009 the Complainant provided my office with copies of records from her injury claim file which she received through an access to information request to SGI. Based on some of those records it was possible to determine who had been granted user access privileges for the Complainant's electronic injury claim file. In my investigation, I determined the following:

- On February 5, 2007 Regina Injury Claims Centre opened an electronic and paper injury claim file. At that time, the following had the ability to access the Complainant's personal information and/or personal health information:
    - All Personal Injury Representatives (PIR) in all Injury Claims Offices in Saskatchewan;
    - Clerks in all branches; and
    - All Claims Administrative personnel.

- On February 13, 2007 access restrictions were put in place. The Complainant's manager sent a request to Claims Support Services (Claims Administrative personnel) and requested that access be restricted to nine individuals plus claims administrative personnel who were responsible for setting up the user access privileges. The nine individuals included three of the Complainant's work colleagues from her unit, her manager, supervisor, an independent adjuster (external to SGI), clerical staff, the Assistant Vice President and the manager of Claims in Head Office.

- On February 14, 2007 the Complainant's injury claim file was transferred to Saskatoon Claims Centre for ongoing maintenance. On the same date, a supervisor at the Saskatoon Claims Centre requested the Complainant's manager in Regina arrange for user access to the electronic injury file for three Saskatoon Injury Claims Centre staff. The Complainant's manager made the request internally via email to Claims Support Services listing the three additional users. It did not appear that the nine employees previously granted access in the Regina Claims Centre were removed at this time.

- On March 13, 2007 a Saskatoon Personal Injury Representative requested that five more individuals be granted user access privileges. The roles of four of these individuals were not clarified for my office by SGI.

- On February 17, 2008 the Complainant, being concerned about who had access to her electronic injury claim file sent an email to the independent adjuster asking him to identify all who had user access privileges.

- On February 20, 2008 a Saskatoon supervisor requested three individuals be removed from having user access privileges: the Complainant's manager, the Complainant's supervisor and the Assistant Vice President from Head Office.

- On February 21, 2008 the independent adjuster emailed the Complainant and told her who had access to her electronic injury file. The three individuals removed the day before were not included in the list provided to the Complainant. It is not clear why SGI chose to remove these individuals before responding to the Complainant's request.

- From February 21, 2008 to February 23, 2009 several more individuals were added and removed from having user access to the Complainant's electronic injury claim file. However, the roles of several of the individuals were not clarified for my office by SGI.

III ISSUES

1. Which Acts are engaged in this case?

2. Is there "personal information" and "personal health information" involved as defined by *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?

3. Did SGI "use" the personal information and personal health information in accordance with section 28 of *The Freedom of Information and Protection of Privacy Act* and section 26(3) of *The Health Information Protection Act*?

IV DISCUSSION OF THE ISSUES

1. Which Acts are engaged in this case?

[10] SGI is a "government institution" as defined in section 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP)[1] and is therefore subject to the Act as it relates to "personal information."[2]

[1]*The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (hereinafter FOIP) at section 2(1)(d)(ii).
[2]This has also been determined in previous Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC) Review Reports F-2006-005 and F-2007-002 and Investigation Reports F-2010-001 and H-2004-001, available at www.oipc.sk.ca/reviews.htm.

[11] SGI is also a "trustee" as defined in section 2(t)(i) of *The Health Information Protection Act* (HIPA)[3] and is therefore also subject to that Act as it relates to "personal health information."[4]

[12] It appears that there are two activities by SGI involved on the facts in this case: (1) the adjudication of the Complainant's injury claim; and (2) the return-to-work (RTW) planning with the Complainant's employer (also SGI).

[13] Given the potential application of paramountcy provisions in FOIP and HIPA, this Report will separate these two activities from this point forward.

(a) Paramountcy as it relates to the adjudication of the injury claim

[14] For the purposes of its work, SGI relies on *The Automobile Accident Insurance Act* (AAIA)[5] for its authority. Our office has addressed the issue of paramountcy and the AAIA in previous public Reports.[6]

[15] In its submission to our office dated September 7, 2012, SGI stated the following:

> Turning to your office's findings that *The Freedom of Information and Protection of Privacy Act* (hereinafter "FOIP") applies to the collection, use and disclosure of the complainant's personal health information under Part VIII injury file, SGI disagrees with this conclusion. SGI is of the view that your office does not have jurisdiction to investigate SGI's handling of personal information under FOIP.

[16] Section 4 of HIPA states as follows:

> **4**(1) Subject to subsections (3) to (6), where there is a conflict or inconsistency between this Act and any other Act or regulation with respect to personal health information, this Act prevails.

[3] *The Health Information Protection Act* (hereinafter HIPA), S.S. 1999, c. H-0.021 at section 2(t)(i).
[4] This has also been determined in previous SK OIPC Investigation Reports F-2010-001 and H-2004-001, available at www.oipc.sk.ca/reviews.htm.
[5] *The Automobile Accident Insurance Act*, S.S. 1978, c. A-35.
[6] SK OIPC Investigation Reports H-2004-001 at [24] to [28] and F-2010-001 at [16] to [36], available at www.oipc.sk.ca/reviews.htm.

> (2) Subsection (1) applies notwithstanding any provision in the other Act or regulation that states that the provision is to apply notwithstanding any other Act or law.
>
> (3) Except where otherwise provided, *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* do not apply to personal health information in the custody or control of a trustee.
>
> **(4) Subject to subsections (5) and (6), Parts II, IV and V of this Act do not apply to personal health information obtained for the purposes of:**
>
> …
>
> **(b) Part VIII of *The Automobile Accident Insurance Act*;**
>
> …
>
> (5) Sections 8 and 11 apply to the enactments mentioned in subsection (4).
>
> (6) ***The Freedom of Information and Protection of Privacy Act*** **and** ***The Local Authority Freedom of Information and Protection of Privacy Act*** **apply to an enactment mentioned in subsection (4) unless the enactment or any provision of the enactment is exempted from the application of those Acts by those Acts or by regulations made pursuant to those Acts.**[7]
>
> [emphasis added]

[17] Section 4(4)(b) of HIPA removes Parts II, IV and V of HIPA from applying to personal health information that has been collected, used or disclosed where that information was obtained for the purpose of Part VIII (Bodily Injury Benefits) of the AAIA.

[18] This is consistent with what I found in my previous Investigation Report F-2010-001 also involving SGI:

> [16] I considered the relevant law applicable to SGI's work in addressing claims for compensation under AAIA in my Investigation Report H-2004-001. In that case, the complainant objected to the scope of personal health information solicited and collected by SGI that ante-dated the date of the accident. In that Report, I concluded that the relevant law would be FOIP. I further found that in the particular circumstances of the injury and the claim, it was not unreasonable for SGI to solicit and collect the additional personal information. I found however that SGI was bound by section 16 of HIPA and that it had not met its obligations to develop appropriate policies and procedures to avoid excessive collection of personal health information.

[7] *Supra* note 3 at section 4.

> I recommended that SGI confirm to the Complainant and our office that all medical information not directly relevant to making an entitlement decision regarding injuries claimed by the Complainant be removed from its records.
> …
>
> [26] I note that section 4(4)(b) of HIPA makes Parts II, IV and V of HIPA inapplicable to personal health information obtained for the purposes of Part VIII of the AAIA.[8]

[19] Therefore, Parts II, IV and V of HIPA do not apply as it relates to the Complainant's personal health information collected, used and/or disclosed by the insurer (SGI) for the purpose of Part VIII of the AAIA.

[20] However, the remaining Parts of HIPA still apply including section 16 that requires a trustee to have appropriate administrative, technical and physical safeguards in place to protect personal health information. This will be relevant later in this Report.

[21] Where HIPA does not apply to the personal health information FOIP will apply and the information would be treated as personal information instead. This is further explained in my Investigation Report F-2010-001:

> [26] I note that section 4(4)(b) of HIPA makes Parts II, IV and V of HIPA inapplicable to personal health information obtained for the purposes of Part VIII of the AAIA. I further note that sections 35 and 72 of the AAIA that are engaged in this analysis are found in Parts II and VI of AAIA respectively and not in Part VIII. It is not clear that personal health information of claimants that was obtained for the purpose of sections 35 and 72 should be interpreted as personal health information obtained for the purposes of Part VIII and thus excluded from HIPA. I do not however need to resolve that question given my findings and recommendations in this Report.
>
> [27] There was a clear intention by the Legislative Assembly that two different laws (FOIP and HIPA) would not apply to the same personal information at the same time. There was an obvious need to clarify which laws applied to what information and at which times. This clear intention is manifest in section 4(4) of HIPA.
>
> [28] There also was a clear intention by the Assembly to ensure that if HIPA did not apply by reason of section 4(4) of HIPA that FOIP would apply. This would avoid a gap in terms of privacy protection. This intention was manifest in section 4(6) of

[8]SK OIPC Investigation Report F-2010-001 at [16] and [26], available at www.oipc.sk.ca/reviews.htm.

HIPA. It would have been a simple matter for the Legislative Assembly to include in FOIP or HIPA, or regulations under either statute, a provision to the effect that the personal information collected, used or disclosed by SGI in the course of its work under the AAIA would be made exempt from the application of FOIP and HIPA. Such a provision is arguably what is contemplated by section 4(6) of HIPA. No such exemption provision has been enacted as of this date.

[29] To this point, I understand that our analysis is no different than that of SGI.

[30] SGI however then considers section 24(1.1) of FOIP and contends that this section constitutes the 'exemption' authorized by section 4(6) of HIPA. Section 24 of FOIP defines personal information for the purposes of FOIP. Section 24(1.1) provides as follows:

> "Personal Information" does not include information that constitutes personal health information as defined in *The Health Information Protection Act*.

[31] My view is that the purpose of section 24(1.1) of FOIP is to ensure that two different laws do not apply to the same information at the same time. The practical effect of section 24(1.1) is that if personal health information is in the custody or control of a trustee and therefore subject to HIPA, it cannot simultaneously be personal information subject to FOIP. The purpose of the Legislative Assembly in enacting section 24(1.1) was presumably to avoid duplication in legislative coverage, not to create a void where no privacy law applied to the information collected, used and disclosed by SGI in the course of its work under the AAIA. To deny the important rights of Saskatchewan residents prescribed by FOIP and HIPA would warrant clear and unambiguous language that evidenced that the Assembly had turned its mind to such a result. The obvious and appropriate place to do so would have been the paramountcy provision in section 23 of FOIP or the paramountcy provision in *The Freedom of Information and Protection of Privacy Regulations*, section 12.

[32] FOIP and HIPA are quasi-constitutional laws according to the Supreme Court of Canada. They define fundamental rights of Saskatchewan residents and this includes the privacy interest that has been judicially determined to be protected by sections 7 and 8 of the *Charter of Rights and Freedoms*.

[33] As I have noted before, my office follows section 10 of *The Interpretation Act* and the 'modern principle' of statutory interpretation in our oversight role. Since the legislature has not incorporated a purpose or object clause in FOIP, I have been largely guided by the Saskatchewan Court of Appeal and its direction that "[FOIP's] basic purpose reflects a general philosophy of full disclosure unless information is exempted under clearly delineated statutory language. There are specific exemptions from disclosure set forth in the Act, but these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." Obviously, this was said in respect to a formal request for access under Parts II and III which is not the case in these three subject files.

[34] In this regard, I also note that *An Overarching Personal Information Privacy Framework for Executive Government* (Privacy Framework) has not been rescinded so it therefore appears to continue in full force and effect for the current Government. In the roll-out of the Privacy Framework, provincial government employees were advised as follows:

> **Vision: To build a culture of privacy**
>
> **The Vision talked about in the Framework is "To build a culture of privacy". This vision focuses on how we can create a corporate culture within government that reflects greater concern over how we collect, use, disclose, and protect personal information. This puts a much greater emphasis on a citizen's right to have their personal information protected.**

[35] At page 6 of the Privacy Framework it is stated that:

> This Privacy Framework is designed to place Saskatchewan at the strongest possible privacy protection policy position, while balancing the Government's need to meet its public policy obligations.

[36] For all of those reasons, I find that the applicable law is FOIP and more particularly Part IV of FOIP and its protection of privacy provisions.[9]

[emphasis added]

(b) Paramountcy as it relates to the employers RTW planning

[22] What is critical to differentiate in this case is the point where SGI no longer is acting as the Complainant's insurer but the Complainant's employer.

[23] A RTW plan can be defined as follows:

> **Return to Work plan:** a planned process to manage the impact of an individual injured worker's injury, including the documentation of the specific alternate or modified work identified and provided to him/her.[10]

[24] In its submission to our office dated September 7, 2012, SGI stated the following:

[9] *Ibid.* at [26] to [36].
[10] WorkSafe Saskatchewan *Fact Sheet: WCB Standard RTW Definitions (Section 1.4)*, available at www.worksafesask.ca/Default.aspx?DN=e28b1c6e-b77b-46f3-951e-11f7dddadc8b.

> It is noted that your office concluded that all provisions of HIPA are applicable to the return to work issue. Respectfully, SGI disagrees. The collection, use and disclosure of [the Complainant's] personal health information, in regard to the return to work, is authorized under the authority of Part VIII of the AAIA. In the administration of injury benefits for motor vehicle accidents, a critical component of that program concerns the rehabilitation of the customer. Frequently, part of a rehabilitation program involves a return to work program with the customer's employer. Although, SGI in this case, is both the administrator under the AAIA and [the Complainant's] employer, this does not change the statutory authority for the collection, use or disclosure of the personal health information. In its capacity as administrator of the AAIA, SGI collected, used and, to a very limited extent, disclosed [the Complainant's] medical information to SGI, [the Complainant's] employer, in the course of administering a return to work program as part of her injury file.

[25] It appears that SGI is asserting that it can rely on the authority under Part VIII of the AAIA when it is performing its duties as an employer.

[26] Section 23 of FOIP states as follows:

> **23**(1) Where a provision of:
>
> (a) any other Act; or
>
> (b) a regulation made pursuant to any other Act;
>
> that restricts or prohibits access by any person to a record or information in the possession or under the control of a government institution conflicts with this Act or the regulations made pursuant to it, the provisions of this Act and the regulations made pursuant to it shall prevail.
>
> (2) Subject to subsection (3), subsection (1) applies notwithstanding any provision in the other Act or regulation that states that the provision is to apply notwithstanding any other Act or law.
>
> (3) Subsection (1) does not apply to:
>
> (a) *The Adoption Act, 1998*;
>
> (b) section 27 of *The Archives Act, 2004*;
>
> (c) section 74 of *The Child and Family Services Act*;
>
> (d) section 7 of *The Criminal Injuries Compensation Act*;
>
> (e) section 12 of *The Enforcement of Maintenance Orders Act*;

(e.1) *The Health Information Protection Act*;

(f) section 38 of *The Mental Health Services Act*;

(f.1) section 91.1 of *The Police Act, 1990*;

(g) section 13 of *The Proceedings against the Crown Act*;

(h) sections 15 and 84 of *The Securities Act, 1988*;

(h.1) section 61 of *The Trust and Loan Corporations Act, 1997*;

(i) section 283 of *The Traffic Safety Act*;

(j) subsection 10(6) of *The Vital Statistics Act*;

(j.1) section 12 of *The Vital Statistics Administration Transfer Act*;

(k) sections 171 to 171.2 of *The Workers' Compensation Act, 1979*;

(l) any prescribed Act or prescribed provisions of an Act; or

(m) any prescribed regulation or prescribed provisions of a regulation;

and the provisions mentioned in clauses (a) to (m) shall prevail.[11]

[27] Further, with regards to section 23(3)(l) above, section 12 of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations) states the following:

> **12** For the purposes of clause 23(3)(l) of the Act, the following provisions are prescribed as provisions to which subsection 23(1) of the Act does not apply:
>
> (a) section 178 of *The Election Act, 1996*;
>
> (b) section 75 of *The Vital Statistics Act, 2009*;
>
> (c) section 43 of *The Occupational Health and Safety Act, 1993*;
>
> (d) Part III of *The Revenue and Financial Services Act*;
>
> (e) all of *The Income Tax Act* and *The Income Tax Act, 2000;*
>
> (f) section 32 of *The Safer Communities and Neighbourhoods Act;*

[11] *Supra* note 1 at section 23.

(g) section 14 of *The Enforcement of Maintenance Orders Act, 1997*;

(h) section 415 of *The Credit Union Act, 1998*;

(i) section 85 of *The Real Estate Act*;

(j) section 10.1 of *The Saskatchewan Insurance Act*

(k) section 12 of *The Vital Statistics Administration Transfer Act;*

(l) section 61 of *The Mortgage Brokerages and Mortgage Administrators Act*;

(m) section 61 of *The Payday Loans Act.*[12]

[28] There is no paramountcy afforded to the AAIA in section 23 of FOIP or section 12 of the FOIP Regulations. Where SGI is acting as the employer for the Complainant and is engaged in the activities of collection, use and/or disclosure of the Complainant's personal information for the purpose of RTW planning, FOIP applies.

[29] Further, all Parts of HIPA apply where SGI is acting as the employer for the Complainant and is engaged in the activities of collection, use and/or disclosure of the Complainant's personal health information for the purpose of RTW planning. An employer's activities in this regard are not captured under Part VIII of the AAIA. This section applies to SGI as an insurer and not as the employer.

[30] Section 26(3) of HIPA is relevant in this regard:

> (3) **Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent**.[13]
>
> [emphasis added]

[12] *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1 at section 12.
[13] *Supra* note 3 at section 26(3).

[31] I have stated previously that given the prejudice that attaches to the use of personal health information for employment purposes, **express** consent should always be required for section 26(3) of HIPA.[14]

[32] Therefore, in summary the following applies in this case:

Injury Claim File

- All Parts of FOIP applies to the personal information collected, used and/or disclosed as it relates to the adjudication of the Complainant's injury claim file.
- Parts II, IV and V of HIPA have no application relating to the adjudication of the Complainant's injury claim file.
- The remaining Parts of HIPA apply.

Employer's RTW Planning

- All Parts of FOIP apply to the personal information collected, used and/or disclosed as it relates to the RTW plan.
- All Parts of HIPA apply to the personal health information collected, used and/or disclosed as it relates to the RTW plan.

2. Is there "personal information" and "personal health information" involved as defined by *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*?

[33] The definition of "personal information" is in section 24 of FOIP which provides as follows:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

[14]SK OIPC *Report on The Health Information Protection Amendment Regulations, 2010* at p. 7; *Glossary of Common Terms: The Health Information Protection Act*; *2010-2011 Annual Report* at p. 19, available at www.oipc.sk.ca.

(a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
(b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) **Repealed.** 1999, c.H-0.021, s.66.

(d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in The Health Information Protection Act;

(e) the home or business address, home or business telephone number or fingerprints of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

(1.1) "Personal information" does not include information that constitutes personal health information as defined in The Health Information Protection Act.

(2) "**Personal information**" does not include information that discloses:

> (a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;
>
> (b) the salary or benefits of a legislative secretary or a member of the Executive Council;
>
> (c) the personal opinions or views of an individual employed by a government institution given in the course of employment, other than personal opinions or views with respect to another individual;
>
> (d) financial or other details of a contract for personal services;
>
> (e) details of a licence, permit or other similar discretionary benefit granted to an individual by a government institution;
>
> (f) details of a discretionary benefit of a financial nature granted to an individual by a government institution;
>
> (g) expenses incurred by an individual travelling at the expense of a government institution.
>
> (3) Notwithstanding clauses (2)(e) and (f), "**personal information**" includes information that:
>
> (a) is supplied by an individual to support an application for a discretionary benefit; and
>
> (b) is personal information within the meaning of subsection (1).[15]

[34] The definition of "personal health information" is in section 2(m) of HIPA which provides as follows:

> **2** In this Act:
> …
>
> (m) "**personal health information**" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;

[15] *Supra* note 1 at section 24.

> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> > (A) in the course of providing health services to the individual; or
> >
> > (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;[16]

[35] On June 10, 2009 the Complainant provided a submission to my office. The submission included samples of the type of information on her claim file. Included was a copy of an *Occupational Therapist Ergonomic Assessment Report* and an *Injury Claim Summary Sheet*.

(a) Personal information as it relates to the Injury Claim

[36] An example of the type of information in the *Occupational Therapist Ergonomic Assessment Report* is as follows:

> Client: [Complainant's name]
> Date of Birth: [Complainant's date of birth]
> Date of Loss: [Date of loss]

[37] An example of the type of information in the *Injury Claim Summary Sheet* is as follows:

> Pain and stiffness in joints (knees, wrists and ankles), also back, neck, shoulders and ankles now ok. Other injuries improving.

[38] As noted earlier, where HIPA does not apply FOIP will and the personal health information would be treated as personal information under FOIP.

[16] *Supra* note 3 at section 2(m).

[39] Therefore, even though this type of information would normally be personal health information under HIPA, when it is used by SGI as insurer for the injury claim it would be treated as personal information under FOIP. This is due to the paramountcy provisions noted earlier.

(b) Personal information as it relates to RTW planning

[40] When SGI is functioning in the role of employer for the purpose of RTW planning all Parts of FOIP and HIPA are engaged.

[41] The above examples qualify as personal health information under section 2(m)(i) of HIPA. It is assumed that there are many more examples of personal health information in the Complainant's injury claim file.

[42] Therefore, there is both personal information and personal health information involved in this case.

3. Did SGI "use" the personal information and personal health information in accordance with section 28 of *The Freedom of Information and Protection of Privacy Act* and section 26(3) of *The Health Information Protection Act*?

[43] On the facts of this investigation, the "collection" and "disclosure" of the Complainant's personal information and personal health information for the purpose of the adjudication of the injury claim and RTW plan does not appear to be in issue. Therefore, this Report will focus on "use" only.

[44] I defined "use" in my Investigation Report F-2009-001 as follows:

> [78] In any event, section 28 relates to "use" of personal information under its control without consent yet the sharing of information by WCB with E.T. would have been a "disclosure". In my 2008-2009 Annual Report, I defined the terms as follows:
>
> …

> "**Use** indicates the internal utilization of personal information by a public body and includes sharing of the personal information in such a way that it remains under the control of that public body."[17]

[emphasis added]

(a) "Use" as it relates to the purpose of the Injury Claim

[45] What appears to be at issue with regards to use as it relates to the insurer adjudicating the injury claim is adherence to the 'need-to-know' and 'data minimization' principles. As well, ensuring adequate safeguards for the protection of personal health information. These issues will be discussed later in this section.

(b) "Use" as it relates to the employer's RTW planning

[46] What appears to be at issue with regards to use as it relates to the employer doing RTW planning is personal information and personal health information being used for a purpose other than that for which it was collected without consent from the Complainant.

[47] As found earlier in this analysis, all Parts of FOIP and HIPA apply in this regard to the use of the personal information and personal health information by SGI for this purpose.

[48] Section 28 of FOIP provides that:

> **28** No government institution shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, **except**:
>
> > (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
> > (b) for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2).[18]

[emphasis added]

[17] SK OIPC Investigation Report F-2009-001 at [78], available at www.oipc.sk.ca/reviews.htm.
[18] *Supra* note 1 at section 28.

[49] The relevant section of HIPA with regards to use and the matter before us is section 26(3) which states the following:

> **26**(3) **Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent**.[19]
>
> [emphasis added]

[50] The Complainant provided a submission to our office on June 10, 2009. The Complainant expressed concerns about personal information and personal health information collected by SGI for the injury claim file being used for the RTW plan. The Complainant felt that this was occurring in ways that would not normally occur from her experience as a Personal Injury Representative with SGI:

> 13. April 4, 2007: **Occupational Therapist Ergonomic Assessment Report** from [name of company] (an independent vocational rehab company). **A copy of the full report was provided to my manager and supervisor by either [independent adjuster] or [SGI consultant]** of Employee Health and Wellness. I feel only the recommendations should have been provided. **I was questioned about different aspects of the report by my manager** (such as how she would be able to tell if a person "really" wore progressive lenses) **and later noted the report in the file [the Complainant's supervisor] had regarding me, during a meeting I had with her.**
> …
>
> 16. May 29, 2007: **File note by [Saskatoon Personal Injury Representative] regarding my very detailed secondary assessment report from [company name].**
>
> *****I sent an email to [Saskatoon Personal Injury Representative] advising he did not have my permission to release the full report to my manager as he had advised me by telephone she had/or would request it. As a PIR we are "never" allowed to release this report to an employer**.
>
> ******following this conversation and three meetings with my manager during which she requested a copy of the report from me the accommodation did not get arranged** and I was taken off work by medical care providers in late June 2007…
> …

[19] *Supra* note 3 at section 26.

> 18. November 1, 2007: SGI Return to work Plan – please refer to the middle of page 2 which is bolded and indicates **an accommodation for me of 10 additional weekly counselling sessions with the Primary Psychologist**. **This was forwarded by [SGI consultant] of Employee Health and Wellness (SGI Head Office) to my supervisor [name removed]. I was then asked to meet with [supervisor] to sign the plan (see page 3). I do not feel this was appropriate information to include in a return to work plan that goes to my employer.**
> 19. November 20, 2007: file note from [independent adjuster] regarding his telephone discussion with **[SGI consultant] of SGI's Employee Health and Wellness. She had been asked by No Fault to do a RTW plan for me. Following this discussion she called me to advise that she had arranged an "intervention/meeting" with my manager, my supervisor, [independent adjuster], herself and me. [The independent adjuster] was going to advise my manager and supervisor of all of his concerns regarding my claim. I was very upset and did not attend. As a PIR, we would never go to the employer to discuss our concerns about the customer's injuries and claims.**
>
> [emphasis added]

[51] In its submission dated October 13, 2009 SGI stated the following:

> 4. In our discussion, concern was raised by your office that SGI's injury file would be made available to SGI's Human Resource Department who would be handling [Complainant's] disability claim. I can assure you that the two Departments do not share files or any file information. To reiterate, SGIs Privacy Policy states:
>
> > Personal information shall not be used or disclosed for purposes other than those which the information was collected, except with the consent of the individual, or as allowed by law.
>
> The consent to collection in the Application for Benefits does not allow SGI's Claims Division to share this information with the Human Resource Department. Furthermore, the medical information on those files is collected for the purpose of adjudicating the claim. Accordingly, SGI's privacy policy prohibits the exchange of information.

[52] SGI appears to acknowledge that personal information and personal health information collected for the injury claim file and then used for the RTW plan would constitute a different purpose and would require the consent of the Complainant to use.

[53] SGI requires the express consent[20] from the employee if it wishes to access the employee's personal health information for any purpose related to the employment of the individual. This language should be reflected more clearly in SGI's Privacy Policy.

[54] Yet from the Complainant's submission it appears that indeed personal information and personal health information was shared between individuals involved in the injury claim file and RTW planning. Personal information and personal health information collected for one purpose (injury claim) was then used for another purpose (RTW) without the Complainant's express consent.

[55] Another example of this can be found in the Injury Note posted by the Saskatoon Personal Injury Representative to the Complainant's electronic injury claim file which states:

> **Injury Note**
> Received a voice message from [independent adjuster] to the effect that **he has some progress notes from [the Complainant's supervisor] to the effect that they feel she has some 'performance issues' such that she might not even be able to do the PIR II job that she demoted to.** As this point, as President of the Union that [the Complainant] belongs to, I do not believe that I can continue to handle this file due to the potential conflict should there ultimately be disciplinary action that [the Complainant] wishes to have the Union deal with for her. Discussed with [manager, Saskatoon Injury Claims Office] that I cannot continue to handle this file and he will have it reassigned. Phoned [independent adjuster] back and informed him that I am no longer handling this issue and I am unable to give him any direction on it. I did not ask, nor did [independent adjuster] tell me, what the performance issues are alleged to be.
>
> **Created** 28-Jan-2008 1:38 PM **By** [Saskatoon Personal Injury Representative]
>
> [emphasis added]

[56] It appears that the Complainant's supervisor shared with the independent adjuster that the Complaint was having performance issues on the job. It is not clear how the Complainant's job performance is relevant and necessary information in order for the

[20] "**Express Consent**" – must meet the requirements of section 6 of HIPA (consent must be related to the purpose for which the information is required; must be informed consent; must be given voluntarily; must not be obtained through misrepresentation or, fraud or coercion).

insurer to process injury claim benefits to the employer. As well, access privileges for the Complainant's manager and supervisor to the injury claim file were still in place during this time frame.

[57] The Complainant provided our office with a copy of her signed SGI RTW Plan. The Complainant's supervisor is listed as the 'Employer Representative' on that plan.

[58] In SGI's submission to our office dated September 7, 2012 it stated that:

> [Independent adjusters] do not supervise the employee whose claim is being adjusted, they do not provide any input into that employee's evaluation as an employee, nor do they work in the same city or building as the staff person whose injury claim is being adjudicated.

[59] It appears then that the Complainant's supervisor would not need to share with the independent adjuster that the Complainant was having work performance issues of the kind that may result in disciplinary action.

[60] The Canadian Human Rights Commission issued a resource titled, *A Guide For Managing The Return To Work* (Guide). The Guide states as follows:

> You are entitled to find out how the employee's medical condition will affect their ability to complete job duties. Note that you are NOT necessarily permitted to obtain a diagnosis of a condition, only details of how the condition may have an impact on the job.
> …
>
> - **Request employee's consent to obtain further medical or health information (if necessary)**
>
> As a supervisor, you have a duty to make informed decisions on accommodation. In order to do this, you need to gather adequate information about the employee's situation, and abide by privacy and human rights laws while doing so.
>
> If you feel you don't know enough about the employee's situation, you need their consent to retrieve additional information. If the employee refuses to cooperate, explain to them that you cannot properly assess their needs and cannot proceed with the accommodation process until you get this information.
> …

Step #2: If necessary, consult with health and medical specialists
In general, supervisors are entitled to receive the following medical information:

- *Information about the employee's current medical condition*

  You are entitled to find out how the employee's medical condition will affect their ability to complete job duties.

- *Prognosis for recovery (if available)*

  You are entitled to know if the condition is temporary or permanent (if the medical professional has this information: sometimes a prognosis cannot be established). If it is a temporary condition, you are permitted to find out how long accommodation might be required.

- *Information on the employee's capabilities for alternative employment*

  If it is determined that the employee is not capable of performing their normal or modified job duties, alternative positions must be considered. You are entitled to know the employee's capacity to perform alternative work.[21]

[61] The Complainant's personal information and personal health information were collected for the purpose of the injury claim and appears to have been used for a secondary purpose - RTW planning.

[62] This constituted a separate use. SGI has not provided its authority under FOIP or HIPA to use the Complainant's personal information and personal health information for a secondary purpose.

[63] In fact, as noted earlier, section 26(3) of HIPA requires express consent from the Complainant when her personal health information is being used by her employer for an employment related purpose.

[64] Therefore, I find that SGI as the employer did not have the authority under FOIP or HIPA to use the Complainant's personal information and personal health information for the secondary purpose of RTW planning.

[21]Canadian Human Rights Commission *A Guide For Managing The Return to Work*, 2007, pp. 12-14.

(c) Issues which relate to both the Injury Claim and RTW planning

Need-to-Know and Data Minimization Principles

[65] For both the personal information and personal health information involved in the injury claim and RTW planning it appears that there are issues related to the 'need-to-know' and 'data minimization' principles.[22]

[66] These two principles underlie section 28 of FOIP and sections 23 and 26 of HIPA. The need-to-know principle means that SGI should collect, use and disclose only on a need-to-know basis. As well, data minimization means that SGI should collect, use or disclose the least amount of identifying information necessary for the purpose.

[67] Section 23 of HIPA directly refers to these principles:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> (3) **Repealed**. 2003, c.25, s.13.
>
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.[23]
>
> [emphasis added]

[68] All of the individuals involved in this case may in some way be engaged in the provision of services provided by SGI. However, SGI has not explained in detail the roles of each of the 43 individuals alleged to have had user access or if they had a legitimate need-to-know the personal information and personal health information of the Complainant.

[22] As referenced also in SK OIPC Review Reports F-2007-001, F-2009-001, LA-2007-002, LA-2010-001 and Investigation Report F-2012-001 available at www.oipc.sk.ca/reviews.htm.
[23] *Supra* note 3 at section 23.

[69] We noted that these two principles were raised as an issue in our notification letter to SGI dated July 17, 2009 which stated:

> More specifically, the following issues have been identified:
>
> - It appears that an excessive number of the complainant's coworkers (over 30), including her supervisor, worked on her claim and/or had access to her personal information in her claim file, [need-to-know]
>
> - Her claim file seems to contain more than just information about the claim including work history and a potentially excessive amount of personal health information [data minimization]
>
> …

[70] In the Complainant's submission to my office dated June 10, 2009 the following is stated:

> Please note that from February 5, 2007 to February 13, 2007 **all Personal Injury Representatives in all Injury Centres in the province would have been able to access my online claim.** I am not suggesting they did as I have no way of knowing this.
> …
>
> 11. March 1, 2007: Email from [SGI employee] to [independent adjuster] dated March 1, 2007 regarding a message from [the Complainant's supervisor]. She was instructing him that practitioner's reports should be put in a sealed envelope with his name on it. This was because **a detailed report regarding my injuries (from [business name removed]) had been opened by clerical staff in our office**.
> …
>
> 18. November 1, 2007: SGI Return to work Plan – please refer to the middle of page 2 which is bolded and indicates **an accommodation for me of 10 additional weekly counselling sessions with the Primary Psychologist**. **This was forwarded by [SGI consultant] of Employee Health and Wellness (SGI Head Office) to my supervisor [name removed]. I was then asked to meet with [my supervisor] to sign the plan (see page 3). I do not feel this was appropriate information to include in a return to work plan that goes to my employer.**
> …
>
> 24. February 19, 2008: Original Letter from [independent adjuster] to me outlining income benefit paid to me by No Fault from September 17 – December 31, 2007. This was sent to my home address.
>
> 25. February 19, 2008: file copy of the original letter sent to me and date stamped by our office was opened and received on February 25, 2008. **This was opened and**

> **placed in my mail tray at work**. I complained about this in an email to [the independent adjuster].
>
> 26. February 28, 2008: Email from me to [independent adjuster] asking how the copy of this letter ended up being directed to my workplace.
> ***in my email I also mention **a cheque that was twice sent to our office, opened by two different clerical staff, placed in a folder with other mail which all PIR's in the office access and brought to my attention by clerical staff. The cheque stub referred to an overpayment for counseling sessions** for [the Complainant]….
>
> [emphasis added]

[71] It should be noted that the Complainant provided copies of the original emails and documents noted above. My office was able to verify these statements against the evidence provided and they appear to be an accurate reflection of the events as they occurred.

[72] If SGI's starting point or default is to allow all Personal Injury Representatives in the province access to the Complainant's online injury claim then there is a problem as this would be in direct conflict with the need-to-know principle.

[73] According to SGI, in its submission received in my office on October 15, 2009, its policy states that:

> Disclosure within the Corporation
> Only employees with legitimate business purposes will have access to personal information and must ensure personal information is securely held.

[74] We have not received a copy of this policy. However, clearly in this case the policy has not been followed as more than those individuals with a legitimate business purpose could have seen the personal information and personal health information that was showing up in the Complainant's mail tray or staff folder.

[75] It is understood that a number of individual's adjudicating an injury claim would have a specific role in the process and there would be some sharing of file information. This would not be in conflict with the need-to-know or data minimization principles.

[76] However, being involved in the injury claim process may not automatically require that each individual involved be given **full access** to all details as all details may not be needed in order to complete their business purpose.

[77] SGI has asserted in its submission received in my office on October 15, 2009 that:

> 1. All staff claims are handled by an office other than the office in which the staff person is employed. As regards injury and general claims, these are assigned to independent adjusting firms.
>
> As you can appreciate, the primary concern in the handling of staff claim and their families is to ensure that employee's claims are adjusted fairly, that SGI's Corporate image is protected and that no undue pressure is placed on adjusting staff attending these claims.
>
> The SGI "Staff Claims Procedures (Auto) [sic] states:
>
> > SGI branch employee's or their immediate family members claims must be reported to and handled by a claims center other than the one in which the employee works…the damage appraisal must be reviewed and approved by the Manager of Appraisals South or North as applicable and the file noted accordingly.
> > …
> >
> > **…the Branch Manager for the branch handling the claim should also arrange for restricted access to only those persons at the branch handling the claim who have a business need to access the file along with the Head office Manager.**
>
> SGI acknowledges that management of this claim (and any other injury claim) requires many individuals to access [Complainant's] file, despite a restricted access rating. These would include mail clerks at all branches, management and supervisory staff at Saskatoon Injury, the injury representative in Saskatoon Injury who was overseeing the handling of her file by the independent adjuster, all individual [sic] in SGI's income calculation unit, all claims administration personal [sic] (who handle access requests), SGI's medical consultants and senior management.
> …
>
> All original documents are retained by SGI, with the independent adjuster keeping a paper copy. Any information sent to SGI by the independent is, as a matter of policy, marked "Personal and Confidential". Access to the paper file would be limited to the mail or filing clerks, the manager, claims supervisor and supervising adjuster in Saskatoon.
> …

> [emphasis added]

[78] It appears that the policy and procedure were not followed as the Complainant's mail was still opened and left in her mail tray and staff joint folders in the Regina Claims Centre where the Complainant worked on multiple occasions. As well, more than just those individuals noted in the 'Staff Claims Procedures' were provided user access to the Complainant's electronic injury claim file (i.e. Regina Claims Centre employees) despite the file being handled in the Saskatoon Claims Centre.

[79] SGI stated in its submission to our office dated September 7, 2012 that:

> Although we appreciate that some staff had the ability to access to her [sic] file that, upon review had no need for access, these staff did not actually access or review her file information.

[80] If there were individuals who did not have a need-to-know they should not have been provided the opportunity to access the information. The fact that those individuals did not apparently access the Complainant's file does not relieve SGI of its responsibility to prevent such potential for unauthorized access.

[81] In summary, too many staff had access to too much personal information and personal health information on the Complainant's injury claim file – some had no demonstrated legitimate need-to-know.

Adequate Safeguards for the Protection of Personal Information and Personal Health Information

[82] For the personal information and personal health information involved in the injury claim and RTW planning it appears that there are issues related to adequate safeguards.

[83] The duty to protect personal health information is provided for in Part III of HIPA. As found earlier in this Report, Part III would apply to both the personal health information involved in the injury claim file and RTW planning.

[84] Section 16 of HIPA states as follows:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) **unauthorized access to or use, disclosure or modification of the information;** and
>
> (c) **otherwise ensure compliance with this Act by its employees**.[24]
>
> [emphasis added]

[85] I detailed the requirements of section 16 of HIPA in my Investigation Report H-2011-001 at paragraphs [91] to [177].[25]

[86] FOIP does not contain the same explicit language noted above; it is my view nonetheless that all government institutions must also have adequate safeguards in place to protect personal information in its possession or control.[26]

[87] As noted earlier, it is a concern that too many individuals had user access privileges to the Complainant's personal information and personal health information in this case.

[88] Most concerning is that from February 5, 2007 to February 13, 2007 the Complainant's electronic injury claim file was accessible by all Personal Injury Representatives in the province.

[24] *Supra* note 3 at section 16.
[25] SK OIPC Investigation Report H-2011-001 at [91] to [177], available at www.oipc.sk.ca/reviews.htm.
[26] As referenced in SK OIPC Investigation Reports F-2012-001 at [89] and F-2007-001 at [32] and [33].

[89] As well, it appears that several of the Complainant's colleagues whom she worked with on a professional basis had access to her electronic injury claim file even when they were not responsible for adjudicating her injury claim.

[90] It is not clear why the Complainant's manager and supervisor were granted user access privileges in February 2007. It appears their access remained intact until at least February 20, 2008. The manager and supervisor were not automatically provided user access privileges consistent with the SGI *Staff Claims Procedure (Auto)* quoted by SGI earlier in this Report. However, they requested user access privileges via email and were provided it in February 2007. This was after responsibility for the injury claim file was transferred to Saskatoon. Removal of the user access privileges did not appear to occur until the Complainant questioned who had user access privileges to her electronic injury claim file on February 17, 2008. At that time, the Complainant's manager and supervisor were removed prior to responding to the Complainant's inquiry.

[91] There is extensive information available on the appropriate management of user access privileges as they relate to personal information and personal health information. One leading authority in this regard is the International Organization for Standardization (ISO).

[92] ISO recommends the following with regards to user access privileges:

> Objective: To ensure authorized user access and to prevent unauthorized access to information systems.
>
> Formal procedures should be in place to control the allocation of access rights to information systems and services.
>
> The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.
> …
>
> Implementation guidance

> The access control procedure for user registration and de-registration should include:
> …
>
> c) checking the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);
> …
>
> i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4).[27]

[93] As noted earlier, SGI appears to take the position that even though there were individuals with user access privileges that did not need such access, those individuals did not decide to access the electronic injury file therefore "no inappropriate access" occurred. As SGI did not clarify the roles of each individual for us we could not independently verify this.

[94] Despite this assertion, section 16 of HIPA requires that the trustee take reasonable measures to prevent unauthorized access to personal health information.

[95] Not regularly reviewing and adjusting user access privileges based on current and legitimate business purposes would suggest weak technical safeguards.

[96] Allowing personal information and personal health information to be exposed in mail trays and staff joint folders multiple times would suggest weak administrative safeguards.

[97] SGI indicated in its submission to our office dated September 7, 2012 that:

> It is unfortunate that mail was addressed incorrectly to [the Complainant's] office. SGI understands [the Complainant's] privacy concerns in this regard. Given that the correspondence was sent in error to [the Complainant's] work address, SGI is of the opinion that this error was handled by our staff as effectively as possible.

[98] This would be a fair assertion had this not occurred multiple times.

[27] ISO Standards, *Information Technology – Security Techniques – Code of practice for information security management*, International Standard ISO/IEC 17799, (2005) at p. 61.

[99] Therefore, SGI did not have reasonable administrative and technical safeguards in place to protect the Complainant's personal information and personal health information in contravention of FOIP and HIPA.

[100] Furthermore, I find that SGI as insurer and employer has not abided by the principles underlying section 28 of FOIP and section 23 of HIPA: the 'need-to-know' and the 'data minimization' principles.

[101] A number of the concerns described in this Report can be attributed to an attitude best captured in SGI's submission to our office referenced below:

> As you can appreciate, the primary concern in the handling of staff claims and their families is to ensure that employees claims are adjusted fairly, that SGI's Corporate image is protected and that no undue pressure is placed on adjusting staff attending to these claims.

[102] This statement seems to be deficient and cast too narrowly. Given SGI's obligations under FOIP, HIPA and the *Overarching Personal Information Privacy Framework for Executive Government*[28] one might reasonably expect that a primary concern would also be protecting the privacy of the employee who may also be a claimant under the AAIA.

[103] This case involves an employee of SGI. If an employer does not have clear rules and restrict access as an employer there is the risk for substantial work related prejudice to the employee.

Agreements and Contracts with External Third Parties Acting on Behalf of a Public Body

[104] Central to the discussion in this regard is the need for agreements and/or contracts between SGI and all external third parties that are providing a service or acting on behalf

[28]See SK OIPC Investigation Report F-2010-001 at [34] and [35], available at www.oipc.sk.ca/reviews.htm and Province of Saskatchewan *An Overarching Personal Information Privacy Framework for Executive Government*, September 2, 2003, available at www.gov.sk.ca/news-archive/2003/9/11-648-attachment.pdf.

of SGI. This would include the external third party performing independent adjuster activities for SGI.

[105] My office has stated in our resource: *A Contractor's Guide to Access and Privacy in Saskatchewan:*

> The Acts apply to all records in the possession or under the control of a public body in Saskatchewan. As a contractor or a potential contractor to a public body, you may produce or store records that will be under the control of that public body. These records are subject to the access and privacy provisions of the respective Acts.
> …
>
> *Possession* of a record usually means having physical custody of it. *Control* refers to having the power or authority to manage, restrict, regulate or administer the collection, use or disclosure of the record.
>
> If a public body has either possession or control of a record, it must respond to requests for access to the record by providing access to those parts of the record that are not exempted from disclosure. **Although a contractor may have possession of a record, a public body could have control over it if such control is stipulated in a contract** or is granted to the public body by a specific statutory right of access. In either case, the public body is responsible for handling access requests, and the contractor is required to produce the record upon request. The public body may disclose those parts of the record that are not exempted from disclosure.
> …
>
> A contract may require you to collect personal information, such as a person's name, address or other information about them. **If you have custody of personal information covered by the Acts, you have an obligation to take reasonable security precautions to protect those records from unauthorized access, collection, use, disclosure or disposal. Information you acquire while under contract can only be used for performing services identified under the contract, and not for any other purpose.**
>
> If the personal information is used to make a decision that directly affects the individual, the records should be retained for at least one year so an application for access can be made.
>
> If records are under the control of a public body, you are required to make them available according to the terms of the contract. The contract may require you to make records available after the contract has ended. Your obligations apply to subcontractors you engage.[29]

[29]SK OIPC *A Contractor's Guide to Access and Privacy in Saskatchewan*, available at www.oipc.sk.ca.

> [emphasis added]

[106] I emphasized the importance of a written agreement with contracted third parties in my Report LA-2010-002:

> [33] **The evidence is that at all material times there was no written contract that particularized the arrangement between the SPS and the City, and that specifically addressed the issue of possession or control of the record.** The City Clerk had never seen the record. The City has contended that it was prejudiced by the delay in this investigation since persons who had direct knowledge of the arrangement between the City and the SPS were not available and that it was necessary to consult with those persons to determine what are or were the terms and conditions of the unwritten agreement with SPS. LA FOIP has applied to the City since 1993. **The City must be taken to have notice that the scope of LA FOIP is broad and that if the City has documents on its premises for purposes of arrangements with outside agencies, it ought to clarify those arrangements by written agreements to accurately reflect the intentions of both parties. Failure to do so runs the risk that is the subject of this review, namely a finding that the City is in possession or control of those records.** This is not a case of records left with the City on some temporary basis or on a basis where the City would have no responsibility whatsoever for the records.[30]
>
> [emphasis added]

[107] With regards to the external third parties (such as the independent adjuster), SGI has not clarified whether there are adequate contracts or agreements in place with any of the external third parties. If there is no agreement or contract, the sharing of the Complainant's personal information and personal health information is considered a "disclosure"[31] which would require the requisite authority under sections 29 of FOIP[32] and 27 of HIPA[33] and when it is for the purpose of RTW planning.

[108] If there is a contract in place with each external third party then the sharing of personal information and personal health information is considered a use by SGI. The contracts

[30]SK OIPC Report LA-2010-002 at [33], available at www.oipc.sk.ca/reviews.htm.
[31]The Commissioner defined "disclosure" in his Investigation Report F-2007-001 at [179] as follows: "**Disclosure** is the sharing of personal information with a separate entity, not a division or branch of the public body or trustee in possession or control of that record/information".
[32]Section 29 of FOIP requires that SGI have consent of the individual in order to disclose outside the organization unless it has authority to disclose without consent under one of the subclauses of section 29(2).
[33]Section 27 of HIPA requires that SGI have consent of the individual in order to disclose outside the organization unless it has authority to disclose without consent. That authority may be found in section 27(2) or (4) or section 29 of HIPA.

and agreements should sufficiently outline the responsibilities of the third parties as they relate to FOIP and HIPA.

[109] One important clause that should be built into a contract or agreement with a third party performing services on behalf of SGI (such as the independent adjusters) is what would happen to the personal information and personal health information used by the third party once the service is complete. This is important because SGI must retain possession/custody and control of personal information and personal health information if it chooses to contract out services to external third parties and without a contract or agreement it is unable to do so.

V FINDINGS

[110] I find that there is personal information and personal health information involved in this case.

[111] I find that all Parts of *The Freedom of Information and Protection of Privacy Act* apply to the personal information of the Complainant for the adjudication of her injury claim and the return-to-work plan.

[112] I find that Parts II, IV and V of *The Health Information Protection Act* do not apply to the personal health information of the Complainant as it relates to the adjudication of her injury claim's file pursuant to the provisions under Part VIII of *The Automobile Accident Insurance Act.* Part III of *The Health Information Protection Act* still applies.

[113] I find that all Parts of *The Health Information Protection Act* apply to the personal health information involved in the return-to-work plan.

[114] I find that Saskatchewan Government Insurance has not abided by the need-to-know and data minimization principles in this case with respect to its use of the Complainant's personal information and personal health information for both noted purposes. This includes the failure to have reasonable administrative and technical safeguards.

[115] I find that a privacy breach has occurred in this case.

VI RECOMMENDATIONS

[116] I recommend that Saskatchewan Government Insurance offer an apology to the Complainant.

[117] I recommend that Saskatchewan Government Insurance review and enhance its user access policies and procedures to ensure compliance with *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* and the need-to-know and data minimization principles to prevent unauthorized access to personal information and personal health information in future similar cases.

[118] I recommend that the Legislative Assembly amend *The Freedom of Information and Protection of Privacy Act* and/or *The Health Information Protection Act* to clarify the rules that will apply to the personal information and personal health information collected, used and disclosed by Saskatchewan Government Insurance in its activities under *The Automobile Accident Insurance Act.* As well, that the role of our office in overseeing Saskatchewan Government Insurance's statutory responsibilities under *The Freedom of Information and Protection of Privacy Act* and/or *The Health Information Protection Act* be clarified.

Dated at Regina, in the Province of Saskatchewan, this 31st day of October, 2012.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner