Chapter 26
Finance—Public Employees Benefits Agency—Securing Personal Information

1.0 Main Points

The Public Employees Benefits Agency (PEBA) operates and administers various government pension and benefit plans for employees of the Government of Saskatchewan and certain employees of municipal governments. PEBA is responsible for maintaining personal information[1] that is required for the operation and administration of these plans.[2] PEBA must secure information entrusted to it.

For the 12-month period ended July 31, 2016, PEBA had, other than for the following matters, effective processes to secure pension and benefit plan participants' personal information.

PEBA needs to make all procedures used to secure personal information readily accessible to its staff to reduce the risk that employees will not follow processes. In addition, PEBA needs to periodically update its non-IT policies to secure personal information. Not doing so increases the risk PEBA may no longer appropriately secure personal information.

2.0 Introduction

PEBA is a branch within the Ministry of Finance. Under *The Financial Administration Act, 1993,* PEBA is responsible for operating and administering various government pension and benefit plans for Government of Saskatchewan employees and certain municipal government employees. PEBA is responsible for creating and maintaining any records, data, and other documents that are required for the operation and administration of these plans.[3]

This chapter describes the results of our audit of PEBA's processes to secure pension and benefit plan **participants**' personal information for the 12-month period ending July 31, 2016.

See **Glossary** in **Section 7.0** for definition of items in **bold** font.[4]

[1] Examples include medical reports, coroner reports, social insurance numbers, marriage certificates, birth certificates, death certificates, and banking information.
[2] *The Financial Administration Act, 1993*, s.64 (1).
[3] Ibid.
[4] The term is in bold font where it is used for the first time in this chapter.

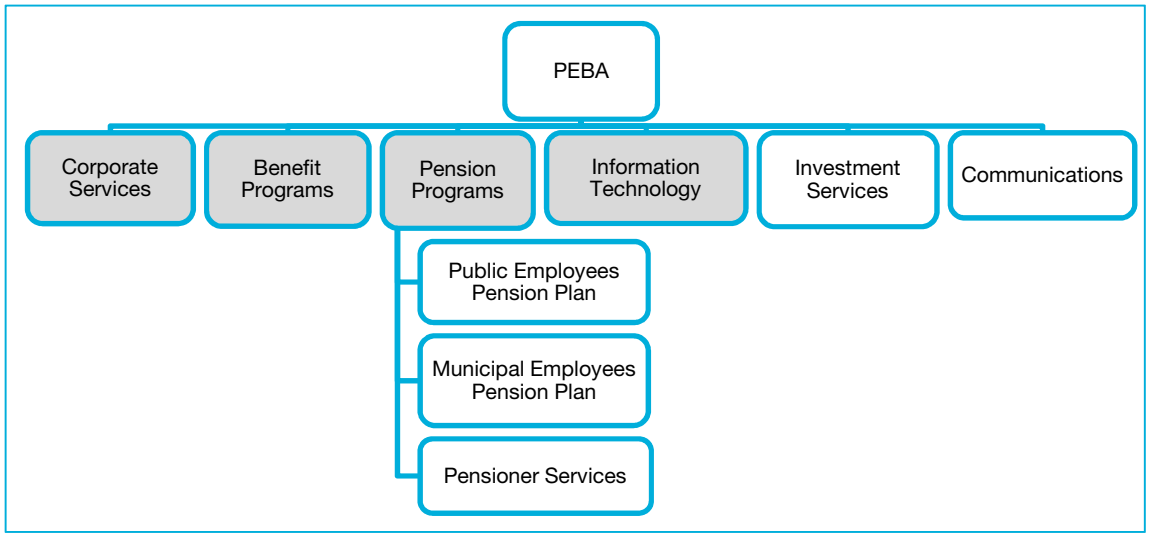
3.0 BACKGROUND

3.1 PEBA Administers Plans

PEBA uses approximately 120 full-time equivalent employees,[5] costing $16.8 million annually,[6] to operate and administer 34 pension and benefit plans (plans). These plans have about 90,000 participants[7] from approximately 1,000 employer groups.[8] See **Section 6.0** for a list of plans. Participants rely on PEBA to properly administer these plans.

As shown in **Figure 1**, PEBA is organized into six program areas, four of which regularly use or have ongoing access to personal information of plan participants (shaded boxes).

Figure 1—PEBA Program Areas at July 2016



Source: Adapted from www.peba.gov.sk.ca/about/PEBA.html (23 August 2016).

To administer the plans, PEBA maintains personal information on each participant in each plan. PEBA stores personal information in physical (e.g., paper files) and electronic formats (e.g., about five computer systems and databases). It also shares certain personal information with third-party service providers it engages (e.g., actuaries used to estimate a plan's pension or benefit obligation). PEBA gives its employees and third-party service providers (users) access to certain participants' personal information to enable them to perform their duties. It varies access granted to the users based on the user's duties.

3.2 Responsibility to Secure Personal Information

PEBA must protect information entrusted to it. It must follow requirements set out in *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Health Information*

[5] Information provided by PEBA management in July 2016.
[6] Public Employee Benefits Agency Revolving Fund Financial Statements for the year ended March 31, 2016.
[7] www.peba.gov.sk.ca/about/peba.html (17 August 2016).
[8] Information provided by PEBA management in July 2016.

Protection Act (HIPA). These laws govern how government institutions (like PEBA) may collect, use and disclose personal information.

FOIP and HIPA establish the rights and obligations respecting access to and protection of **personal information** and **personal health information** (collectively referred to as personal information in this chapter).

PEBA is responsible for securing personal information so that:

- Only those who need the information to perform their duties have access
- Information is not intentionally or inadvertently disclosed to others without consent (except for in prescribed situations; for example, to comply with a subpoena or warrant)
- Information is only used for its intended purpose to administer plans

In addition to the legal requirements to secure personal information, PEBA and its employees must follow:

- *An Overarching Personal Information Privacy Framework For Executive Government*[9] established by the Ministry of Justice. This framework sets the Government's privacy policy expectations and provides a basis for policy development for government agencies.
- *Information Technology Acceptable Usage Policy*[10] established by the Public Service Commission. This policy requires ministry employees to follow guidelines and policies on the usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations, and policies. PEBA employees are employees of the Ministry of Finance.

3.3 Importance of Securing Personal Information

The Canadian Anti-Fraud Centre reported that 17,140 complainants reported losses due to **identity fraud** of $10.8 million between January and November 2015.[11] In addition, the Canadian Anti-Fraud Centre estimates that the total number of complaints, victims, and dollar losses presented in its report represents less than 5% of the total number of actual victims. It suggests losses and victims due to fraud could be much higher.[12]

Breaches of personal information, that Saskatchewan government agencies maintain, can and do occur. For instance, on May 9, 2016, and June 20, 2016, PEBA became aware of instances where it inadvertently mailed a plan participant's personal information to another participant. In another instance, between June 30, 2015 and August 6, 2015, Saskatchewan Government Insurance suffered a privacy breach through a licence issuer affecting 17 people.[13]

[9] http://publications.gov.sk.ca/documents/9/39659-11-648-attachment.pdf (17 August 2016).
[10] www.cs.gov.sk.ca/1103 (17 August 2016).
[11] www.antifraudcentre-centreantifraude.ca/reports-rapports/2015/nov-eng.htm (17 August 2016).
[12] Ibid.
[13] Office of the Saskatchewan Information and Privacy Commissioner, *Investigation Report 131-2015 Saskatchewan Government Insurance*, (2015).

If PEBA does not have effective processes to secure participants' personal information, it increases the risk of loss, misuse, or unauthorized disclosure of personal information. This could lead to theft of a participant's identity for fraudulent purposes. This could also result in significant financial loss by the participant, negatively impact the public's trust in PEBA and the Government of Saskatchewan, and expose the Government to potential litigation.

4.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether PEBA had effective processes to secure pension and benefit plan participants' personal information for the 12-month period ending July 31, 2016.

We did not assess PEBA's processes to secure information shared with third-party service providers (e.g., actuaries), or whether information PEBA collects is accurate and complete.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate PEBA's processes, we used criteria based on related work, reviews of literature including reports of other auditors, and consultations with management. Management agreed with the criteria (see **Figure 2**). We interviewed PEBA management and employees responsible for securing participants' personal information and reviewed related documentation. We tested a sample of employees' access to electronic systems to assess appropriateness, and timely removal of terminated employees' access. We also observed key security monitoring activities.

Figure 2—Audit Criteria

1. **Approve a security framework for personal information**
   - 1.1 Identify personal information
   - 1.2 Evaluate risks to personal information
   - 1.3 Approve security policies and procedures that align with provincial government legislation and risks
2. **Implement security policies and procedures**
   - 2.1 Assign responsibility for security policies and procedures
   - 2.2 Promote security awareness
   - 2.3 Restrict access to personal information based on identified user need
3. **Monitor security of personal information**
   - 3.1 Monitor compliance with approved security policies and procedures
   - 3.2 Report results of monitoring activities to senior management
   - 3.3 Update security policies and procedures for lessons learned (e.g., changes in risk, in response to security breach)

We concluded that, for the 12-month period ended July 31, 2016, PEBA had effective processes to secure pension and benefit plan participants' personal information, except it needs to:

- **Make procedures that are used to secure personal information accessible to its staff**
- **Require periodic updates to its non-IT personal information security policies**

5.0 KEY FINDINGS AND RECOMMENDATIONS

In this section, we set out the criteria (expectations) in italics, and our key findings along with related recommendations.

5.1 Personal Information Identified

*We expected PEBA to determine what personal information it needs to maintain in order to perform its duties, and only maintain information that it needs. We also expected PEBA to have a listing of personal information it maintains. The listing would include where the personal information is stored (e.g., physically in participant files, electronically on **network drives**).*

The information PEBA needs for each plan does not change frequently. PEBA determines what information to maintain based on what information it needs to administer the plans and relevant legislation. For example, to administer the Disability Income Plan (DIP), PEBA needs personal health information to assess whether the reported participant disability qualifies under DIP provisions. In addition, it requires some of the participant's personal information for reporting taxation information under the *Income Tax Act*.

We found that PEBA only maintains personal information required to administer each plan.

In February 2016, PEBA compiled a listing of personal information it maintains.[14] It lists some information on the type of personal information (e.g., Social Insurance Number, banking information, address) for each of its program areas, the format in which the information is stored (physical or electronic), and user access privileges for the information. The listing did not contain the same detail for all information. For example, the listing includes the **network** location (e.g., network drive, pension administration system) for some personal information but not all. However, given PEBA staff demonstrated awareness of personal information PEBA maintains and its location, we found PEBA sufficiently identified personal information. PEBA may find that maintaining a listing with comparable level of detail beneficial in the event of staff turnover.

5.2 Risks to Personal Information Assessed

We expected PEBA to periodically assess risks to personal information it maintains. PEBA would document its risk assessment, have it approved by senior management and have documented risk mitigation plans for key risks it identified.

We found that PEBA effectively assessed risks to personal information it maintains.

Beginning in 2016, PEBA uses an Enterprise Risk Management (ERM) process to annually evaluate and document internal and external threats to achieving its objectives. This process includes identifying various risks, assessing likelihood and impact, and developing risk management strategies.

[14] PEBA refers to this listing as *PEBA Consolidated Listing – Private and Sensitive Information*.

PEBA senior management approved the 2017-18 ERM plan on July 7, 2016. Some of the risks identified in the 2017-18 ERM plan relate to the security of personal information, for example:

- Risk of breach in IT security or issues with IT general controls could result in theft or damage of personal information
- Risk that PEBA may experience an event that would cause its stakeholders and public to view PEBA negatively (e.g., fraud, privacy breach)
- Risk that PEBA does not administer a plan in compliance with the rules, regulations, or fiduciary standards imposed on the plan in any jurisdiction in which the plan operates

In addition, the 2017-18 ERM plan included risk mitigation strategies such as training, documentation of processes, internal controls, security assessments, and increased standardization and automation.

5.3 Certain Security Procedures Need to be Readily Accessible

We expected management to have approved security policies and procedures. Those policies and procedures would include PEBA's definition of personal information. We also expected PEBA's policies and procedures and definition would align with provincial government legislation, central government guidance (e.g., Ministry of Justice), and would respond to PEBA's identified risks.

In April 2016, PEBA documented and approved PEBA-wide security policies and program area-specific security procedures. Management from each of its program areas met between December 2015 and April 2016 to propose security policies and procedures. PEBA's senior management approved its security policies on April 21, 2016. Each of its program areas informally approved program area-specific procedures.

PEBA's security policies and procedures require the safekeeping of personal information within PEBA. Although they do not specifically define personal information, management told us PEBA uses the definitions of personal information provided in FOIP and HIPA.

We found PEBA's policy refers to these Acts. Also, online privacy training provided to new government employees, and training provided by the Ministry of Justice to PEBA employees in February 2016, specifically refers to the FOIP and HIPA definitions of personal information.

In addition, we found PEBA's security policies and procedures aligned with:

- *The Freedom of Information and Protection of Privacy Act*
- *The Health Information Protection Act*
- Agreement for the Administration of the Public Employees Pension Plan
- Agreement for the Administration of the Municipal Employees Pension Plan

PEBA's security policies and procedures also responded to risks identified in PEBA's ERM plan.

PEBA's privacy policy requires its staff to verify a participant's identity using a minimum of two unique pieces of identification verbally or in writing prior to disclosing the participant's personal information. To augment the privacy policy, some of PEBA's program areas have documented procedures for verifying the identity of a participant.

PEBA has not included guidance for providing participants physical access to their personal file in its privacy policy. Rather, informal guidance exists in a 2010 email.

The 2010 email requires PEBA staff, when providing a participant with access to his/her file, to document in the related participant's file the specific information the participant accessed. Also, it suggests, when participants want to give another individual access to his/her file, PEBA staff ask the participant to provide PEBA with written permission for such access. While the 2010 email provides reasonable guidance, the email is not readily available or known to all staff.

Not making expected procedures readily accessible to staff increases the risk that employees are not aware of or will not follow the processes. Also, in the event of employee turnover, knowledge of informal processes could be lost and result in breakdowns in control, which could result in inappropriate disclosure of participant personal information.

1. **We recommend that the Public Employees Benefits Agency maintain its procedures used to secure personal information in a manner that is readily accessible to its staff.**

5.4 Security Awareness Promoted

We expected PEBA to assign responsibilities for implementing security policies and procedures to staff based on their job duties. We expected PEBA would communicate approved security policies and procedures to staff and provide regular security awareness training and reminders to staff.

PEBA assigns responsibility for security policies and procedures to staff based on their job duties. For example, one person is responsible for securing the file room where physical participant files are stored. PEBA also assigns responsibility for some security policies and procedures to all staff. For example, all PEBA staff who deal with personal information are responsible for implementing its clean desk policy, and verifying participant identity before disclosing any personal information.

Management communicates PEBA's approved security policies and procedures to staff through its **intranet**. We found staff were aware of the security policies and procedures and where to find them, with the exception of guidance to provide participants access to their personal file as described in **Section 5.3**. In addition, PEBA requires new staff to complete a mandatory privacy-training course and tracks their attendance. As previously noted, its staff periodically receive privacy training from the Ministry of Justice (e.g., in February 2016).

Each year, PEBA requires its entire staff to confirm, in writing, they are familiar with PEBA's IT security policies and procedures. All staff in our sample confirmed, in writing, their awareness of IT security policies and procedures.

In addition, PEBA's April 2016 privacy policy requires each employee to confirm annually, in writing, awareness of the other (non-IT) privacy policies. As of July 31, 2016, PEBA management had not yet implemented this process. Management told us it plans to require staff to annually confirm their awareness of IT and non-IT security policies and procedures at the same time. It expects to request the first confirmation of awareness of non-IT policies to occur in March or April 2017.

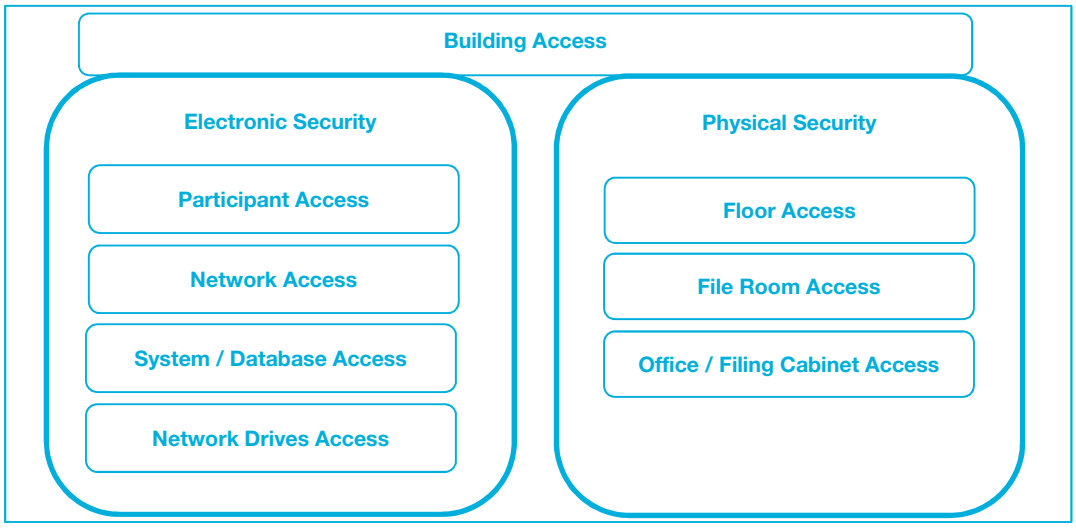
5.5 Access to Personal Information is Appropriately Restricted

We expected PEBA to assign user access based on job position. We expected physical access to the building, floors in the building, and file rooms to be appropriately restricted, and logical access to PEBA's IT network, systems and drives to be appropriately restricted.

PEBA restricts access to physical and electronic information based on user need. **Figure 3** illustrates the levels of security PEBA has in place to secure plan participants' personal information.

PEBA differs employees' access based on their job position, program area, and assigned duties. Semi-annually, PEBA reviews whether it has granted staff with appropriate access to electronic information. Beginning in April 2016, PEBA annually assesses access to physical information provided to each employee through its **access card system**.

Figure 3—PEBA's Levels of Security at July 2016



Source: Developed by Provincial Auditor of Saskatchewan.

PEBA's electronic security measures include:

- Requiring participants to use a unique identifier and password to access their information through the Public Employees Pension Plan (PEPP) Access website
- Using IT controls, such as firewalls, antivirus, and periodic risk and security assessments, to secure its IT network
- Requiring staff to use a unique identifier and password to restrict access to pension administration systems
- Limiting access of staff to folders on network drives, where personal information is stored, based on their assigned duties

PEBA's physical security measures include:

- Using an access card system after business hours and on weekends to restrict physical access to the building; building is only unlocked during weekday business hours
- Using separate access cards, assigned to PEBA staff, to restrict access to PEBA floors (floor access cards)
- Using access cards, assigned to a limited number of select employees, to restrict access to its file rooms and server rooms
- Requiring staff who need a participant file from its file room to request the file from an individual with access to the file room
- Requiring staff to lock their individual office and/or filing cabinet
- Limiting access to copies of office and filing cabinet keys to select employees; and storing these keys in lockboxes, in case an employee with access is not available

Through the following procedures, we found PEBA appropriately restricted access to personal information. We:

- Reviewed IT access restrictions for the PEPP Access website
- Identified and tested IT controls used to secure PEBA's IT network
- Reviewed IT user access listings for pension administration systems, folders within network drives, and floor access cards to assess appropriateness based on job position, program area, and job duties
- Reviewed results of PEBA's most recent floor access card assessment
- Reviewed results of PEBA's semi-annual IT user access assessment
- Tested whether user access was appropriately removed for a sample of terminated employees

5.6 Monitoring of Compliance with Policies and Procedures Ongoing

We expected PEBA to monitor compliance with approved security policies and procedures. It would communicate monitoring processes to responsible staff. We also expected PEBA to follow its monitoring processes.

PEBA has established processes to monitor compliance with its security policies and procedures. For example, it has documented procedures to: track which new employees complete the mandatory online privacy training; daily monitor compliance with its clean desk policy; annually assess the appropriateness of access granted through floor access cards; and assess the appropriateness of access restrictions to the network drive (annually), and pension administration system (semi-annually).

We found that staff is aware of the established monitoring processes. For monitoring activities we tested, PEBA staff followed its established monitoring processes. Through observation, we found staff carried out **clean-desk walkthroughs** as expected.

5.7 Periodic Reports Provided to Senior Management

We expected PEBA to provide senior management with periodic reports on security and to report non-compliance.

PEBA has established processes to report non-compliance with security policies and procedures to the appropriate level of management. PEBA expects staff to take corrective action and verbally report to his/her supervisor instances of non-compliance that did not lead to a privacy breach (e.g., not locking up a participant file at the end of the day detected through a clean-desk walkthrough). PEBA expects supervisors to remind employees, who did not comply, about the policy.

For non-compliance with security policies and procedures breaching privacy, it requires staff to complete a privacy-breach-response checklist. This checklist requires communicating the incident to senior management.

We found that PEBA staff reported non-compliance with security policies and procedures resulting in breach of privacy to senior management as required. For example, between August 1, 2015 and July 31, 2016, PEBA experienced two privacy breaches affecting two pension participants. PEBA became aware it had inadvertently mailed participant personal information to another participant on two separate occasions. For each breach, management completed the privacy-breach-response checklist on a timely basis. PEBA conducted an investigation to determine the underlying cause of the breach, and revised its procedures to mitigate the risk of the situation recurring.

PEBA identified security of personal information as one of its key risks (see **Section 5.2**). While PEBA reports instances of non-compliance, at July 2016, it did not regularly report to senior management on its management of the risk of security of personal information.

PEBA's ERM policy requires reporting to senior management on the status of risk items. At July 2016, management was developing an ERM reporting template for senior management's approval and had plans to commence such reporting in January or February 2017.

5.8 Process to Periodically Update Security Policies Needed

We expected PEBA to have a process to regularly review and update security policies and update procedures for changes in policies.

PEBA's process is to update its policies following a security breach so that it reduces the risk of the breach recurring. At July 2016, PEBA had a process to annually update its IT policies and procedures. However, it did not have an established process to periodically review and update non-IT security policies (e.g., clean desk policy).

Not periodically updating policies for changes in risk, information collected, where information is stored, and other administrative processes increases the risk PEBA may no longer appropriately secure personal information.

2. We recommend that the Public Employees Benefits Agency require periodic review and update of its non-IT security policies to keep personal information secure.

6.0 Pension and Benefit Plans PEBA Administered At July 2016

Pension Plans:	**Benefit Plans:**
Anti-Tuberculosis League Superannuation Plan	Crown Investments Corporation of Saskatchewan Benefits Plan
Capital Pension Plan	Extended Health Care Plan
Judges of the Provincial Court Superannuation Plan	Extended Health Care Plan for Certain Other Employees
Liquor Board Superannuation Plan	Extended Health Care Plan for Certain Other Retired Employees
Members of the Legislative Assembly Benefits	Extended Health Care Plan for Retired Employees
Municipal Employees' Pension Plan	Government of Saskatchewan and Canadian Union of Public Employees Local No. 600-3 and Local 600-5 Benefit Plans' Surplus Fund
Pension Plan for the Employees of the Saskatchewan Workers' Compensation Board	Government of Saskatchewan and Saskatchewan Government and General Employees' Union Benefit Plans' Surplus Fund
Public Employees' Pension Plan	Government of Saskatchewan Scheduled Aircraft Plan
Public Service Superannuation Plan	Government of Saskatchewan Unscheduled Aircraft Plan
Saskatchewan Pension Annuity Plan	Public Employees Deferred Salary Leave Plan
Saskatchewan Transportation Company Employees Superannuation Plan	Public Employees Dental Plan
Power Corporation Superannuation Plan	Public Employees Disability Income Plan
	Public Employees Group Life Insurance Plan
	Saskatchewan Government Insurance Service Recognition Plan
	Saskatchewan Water Corporation Retirement Allowance Plan
	SaskEnergy Retiring Allowance Plan
	SaskPower Designated Employee Benefit Plan
	SaskPower Millennium Plan
	SaskPower Severance Pay Credits Plan
	SaskPower Supplementary Superannuation Plan
	SaskTel Retirement Gratuity Plan
	Water Security Agency of Saskatchewan Retirement Allowance Plan

Source: www.peba.gov.sk.ca/about/peba.html (14 June 2016).

7.0 Glossary

Access Card System – A system used to provide access to secure areas by passing a card containing encoded data over an electronic device.[15]

Clean-Desk Walkthroughs – An employee checks the work area at the end of each day to determine whether staff have locked up all personal information.

Identity Fraud – The actual deceptive use of the identity information of another person (living or dead) in connection with various frauds (e.g., impersonating another person, and misusing debit card or credit card data).[16]

Intranet – A communications network within an organization employing the same technology as the internet.

Network – A group of computers that communicate with each other.

Network Drive – An electronic storage space hosted on a shared server where staff can store electronic records.[17]

Participants – Pension and benefit plan participants include all active, inactive and deferred members, pensioners, surviving spouses, and dependents.

Personal Health Information – Information about a participant with respect to their physical or mental health, health services provided to them, or testing or examination of a body part or bodily substance of the individual.[18]

Personal Information – Information about a participant (e.g., information about family or marital status, disability, an identifying number, address, telephone number, personal health information) recorded in physical or electronic formats.[19]

8.0 Selected References

Auditor General of Prince Edward Island. (2010). *2010 Annual Report, Chapter 4 – Security Assessment – Drug Information System*. Charlottetown: Author.

Province of Saskatchewan. (2003). *An Overarching Personal Information Privacy Framework for Executive Government*. Regina: Author. http://publications.gov.sk.ca/documents/9/39659-11-648-attachment.pdf. (24 May 2016)

Provincial Auditor of Saskatchewan. (2010). *2010 Report – Volume 2, Chapter 8, Finance – Information Technology Security Audit*. Regina: Author.

Provincial Auditor of Saskatchewan. (2010). *2010 Report – Volume 2, Chapter 20, Social Services – Processes to Secure Physical Information*. Regina: Author.

Provincial Auditor of Saskatchewan. (2016). *2016 Report – Volume 1, Chapter 17, Social Services – Protecting Children-in-Care Information in the Linkin System*. Regina: Author.

Provincial Auditor of Saskatchewan. (2016). *2016 Report – Volume 1, Chapter 5, Central Services – Data Centre Security*. Regina: Author.

[15] Adapted from www.yourdictionary.com/access-card (09 September 2016).
[16] www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm (09 September 2016).
[17] www.utas.edu.au/__data/assets/pdf_file/0018/132462/RMU-Information-Sheet-11-Storing-Records-in-Shared-Drives.pdf (09 September 2016).
[18] *The Health Information Protection Act*, s.2.
[19] *The Freedom of Information and Protection of Privacy Act*, s.24.