Chapter 17
Social Services—Protecting Children-in-Care Information in the Linkin System

1.0 Main Points

The mandate of the Ministry of Social Services (Ministry, Social Services) is to support citizens at risk as they work to build better lives for themselves through economic independence, strong families, and strong community organizations. The Ministry assists in these efforts through income support, child and family services, support for persons with disabilities, affordable housing, and by building greater capacity in community-based organizations.[1]

The Child and Family Programs Division (CFP) of the Ministry is responsible for developing, designing, implementing, and maintaining effective programs and services for children in need of protection and their families. CFP is also responsible for the safety and well-being of children in care in Saskatchewan. The Ministry uses its electronic case management system, Linkin, to support the delivery of its programs and services for children in care.

For the 12-month period ended December 31, 2015, the Ministry had, other than the following, effective processes to protect information about children in care in the Linkin system. The Ministry needs to:

- Establish a written plan for updating its Linkin system against known security vulnerabilities; updating addresses security vulnerabilities, which reduces the risk of security breaches.
- Implement a policy requiring prompt removal of unneeded user access to Linkin to reduce the risk of unauthorized access to confidential data.
- Verify the completeness of care provider information entered in Linkin. Accurate information helps ensure children who are in care of the Minister are properly protected and cared for.
- Consistently document its review of Linkin reports designed to identify unusual payments. This documented review increases the likelihood of tasks being completed timely and as expected. It also helps reduce the risk of inappropriate payments being made.

2.0 Introduction

The Ministry has regional staff (such as caseworkers) located across the province. They provide both in-home support to families and out-of-home care to children in need of protection. Out-of-home children are sometimes referred to as children in care as they become the Minister's responsibility when they are removed from their at-risk homes and placed with foster parents or extended family. As the designate of the Minister, the

[1] Ministry of Social Services, *Annual Report for 2014-15*, p. 3.

role of a caseworker is to carry out parental responsibilities for the child in care (e.g., provide a home and protect the child). The primary focus is the best interest of the child in care. The caseworker must ensure that children in care receive quality care.

Providing services to children in care involves collaboration of various Ministry staff (e.g. caseworkers) and outside organizations (e.g., provincial courts, First Nation agencies, community-based organizations) to assess, plan, implement, coordinate, monitor, and evaluate the options and services necessary to meet the child's health and human service needs. As such, it involves case management.

This chapter reports the results of our audit of the Ministry's processes to protect information about children in care contained in its electronic case management system called Linkin. See **Section 5.0 Glossary** for definition of IT terms.

2.1 What is Linkin?

Since 2012, Social Services, (primarily CFP) has used Linkin to help caseworkers provide services to children in care and their families. As of October 31, 2015, Social Services provided services to about 2,260 families, and out-of-home care to about 4,725 children.[2]

Linkin facilitates case management. It captures key information about cases and their status. CFP initiates a case file in Linkin by recording reported information (e.g., from a teacher) about the possibility of a specific child being in an abusive or neglect situation. CFP assigns the case situation to a specific caseworker who determines the facts about the situation in stages (e.g., investigates). Where the caseworker validates the situation and determines an intervention is warranted, the case status is updated in Linkin.

Linkin also helps manage and make payments to foster homes (e.g., care providers). The Ministry pays foster parents or extended family for caring for children that the Ministry has placed into their care. For example, foster parents and extended family receive a monthly education allowance as part of their basic monthly maintenance payment for a child. The education allowance is intended to cover the cost of day-to-day, ongoing expenses associated with school attendance, such as gym clothing, school outings, etc.

Linkin includes the following case-management capabilities; it:

- Performs and tracks intake of children into Ministry care
- Creates and tracks ongoing cases and investigations
- Produces case-related forms, templates, and reports
- Enrols care providers (e.g., foster families) and tracks children with providers

Linkin holds personal information related to each child in care (e.g., who they are, where they live [e.g., with foster parents or extended family]) along with other key information (e.g., care plans for the child, court orders). It holds information that the Ministry has accumulated since 2012 (the year of implementation of Linkin). Prior to using the Linkin

[2] Figures based on Ministry of Social Services financial and operational records as of October 31, 2015.

system, the Ministry used paper-based case management files. The Ministry continues to maintain some paper-based files for information pre-dating the use of Linkin.

In November 2015, the Ministry implemented the financial component to Linkin.[3] This component generates and tracks payments to care providers (i.e., foster parents and extended families). The financial component of Linkin interfaces with the Government's key financial system[4] that issues the payment (e.g., cheque or electronic fund transfer), and records the payment in the Ministry's financial records. Each year, the Ministry expects to process about $90 million for payments to foster parents and extended families for children in their care through Linkin.[5]

2.2 Importance of Protecting Information in the Linkin System

The Ministry must keep personal and financial information about children in care that is held in Linkin safe from unauthorized and inappropriate access. Inadequate controls to protect the information about children in care could result in:

- Loss or misuse of personal information
- Corruption or manipulation of the information (i.e., impact the accuracy of the information)
- Fraudulent or inaccurate financial payments
- Loss of the public's trust in the Ministry's ability to protect children in its care

3.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether the Ministry of Social Services had effective processes to protect information about children in care in the Linkin system for the 12-month period ending December 31, 2015.

Protecting information about children in care means that the information is accessed only by those who need it to perform their duties, and it is not corrupted or lost, either intentionally or inadvertently.

We examined the Ministry's policies, procedures, processes, agreements, reports, and other relevant documents related to the Linkin system. We examined how the Ministry administers using Linkin services and payments for children in care with extended families and foster families. We sampled Linkin system changes, evaluated system settings, and evaluated Linkin system users and roles. We also interviewed various Ministry staff.

[3] Prior to implementation of the financial component of Linkin, the Ministry processed these payments through its family youth assistance program (FYAP) IT system.
[4] Multi-Informational Database Applications System (MIDAS) financials includes modules for general ledger, cash management, accounts payable, accounts receivable, purchasing, payments, forecasting, capital assets, and inventory. It accounts for financial transactions of government ministries. The Ministry of Finance owns and administers this application.
[5] Figures are based on Ministry of Social Services financial and operational records at October 31, 2015.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate the Ministry's processes, we used criteria based on our related work, reviews of literature including reports of other auditors, and consultation with management. The Ministry's management agreed with the criteria (see **Figure 1**).

Figure 1—Audit Criteria

1.	**Set security requirements for Linkin system and data**
1.1	Responsibilities to secure the system and data are clearly defined
1.2	Approved security policies and procedures in place based on data classification
1.3	System is monitored and security issues addressed
2.	**Protect the Linkin system and data from unauthorized and inappropriate access**
2.1	Logical access controls protect the system and data from unauthorized or inappropriate access (including adequate segregation of roles)
2.2	Physical security controls protect the system and data from unauthorized access
3.	**Maintain the integrity of the Linkin system and data**
3.1	Validation processes exist and are followed (e.g., data entry controls)
3.2	Change management processes exist and are followed
3.3	Incident management processes exist and are followed

We concluded, for the 12-month period ended December 31, 2015, the Ministry of Social Services had, other than the following areas, effective processes to protect information about children in care in the Linkin system. It needs to:

- **Establish a written plan for securing its Linkin system against known security vulnerabilities**
- **Implement a policy requiring prompt removal of unneeded user access to Linkin**
- **Verify the completeness of care provider information entered in Linkin**
- **Consistently document its review of Linkin reports designed to identify unusual payments**

4.0 Key Findings and Recommendations

In this section, we describe our key findings and recommendations related to the audit criteria in **Figure 1**.

4.1 Plan Needed for Addressing Linkin Security Vulnerabilities

The Ministry is responsible for the security of the Linkin system (which is an IT database and application) and its data. It recognizes that the security of the Linkin system is impacted by the adequacy of the security of the computer network in which the Linkin system resides, and the security of Linkin's connections with other computer systems (interfaces).

As shown in **Figure 2**, we found the Ministry has entered into agreements with others to clarify security responsibilities related to the Linkin system and its data.

Figure 2—Key Parties with Responsibilities related to Security of Linkin

Linkin system and data	Party responsible and why	Where responsibility is defined
Users of data in Linkin	A First Nations Agency and Ministry of Social Services staff	For the First Nations Agency, agreement between the Agency and Social Services - makes the First Nations Agency responsible for adhering to Social Services security policies and practices. Social Services staff are responsible for adhering to IT policies (e.g., acceptable use policy) and carrying out their assigned roles.
Linkin application and data	Ministry of Social Services – owner of the Linkin application	Memorandum of Understanding between Social Services and Central Services - makes Social Services responsible for following Central Services' security policy. This policy makes Social Services responsible for the security of its applications (such as Linkin) and related data.
Linkin database	Ministry of Central Services - contracted by Ministry of Social Services to manage the Linkin database	Memorandum of Understanding between Social Services and Central Services – Central Services agrees to provide database services for Linkin to Social Services.
IT infrastructure that supports Linkin (e.g., server, computer network, perimeter security)	Ministry of Central Services – contracted by Ministry of Social Services to host the servers on which Linkin resides. These servers reside in a data centre operated by a private IT service provider that Central Services has engaged.	Memorandum of Understanding between Social Services and Central Services – Central Services agrees to provide network and data centre services to Social Services.
Interface of Linkin with MIDAS Financials (another IT system)	Ministry of Social Services – as owner of Linkin Ministry of Finance – as owner of MIDAS Financials	Data Sharing Agreement - Social Services and Finance signed an agreement in December 2015. This agreement sets out terms and conditions for sharing certain Linkin data.

Source: Provincial Auditor of Saskatchewan, 2016, based on agreements related to Linkin.

Also as noted in **Figure 2**, Social Services through its Memorandum of Understanding with the Ministry of Central Services (Central Services), is responsible for complying with Central Services' IT policies including its security policy and data classification policy.

Central Services' data classification policy requires ministries to consider the sensitivity and confidentiality of data, and places differing security requirements based on the data classification. Because Linkin contains highly sensitive confidential and personal information including social insurance numbers, health numbers, birthdates, and case information, the Ministry has classified the data in Linkin as Class A data.[6] We found that it had incorporated the security requirements for Class A data into the design of the Linkin system (e.g., inclusion of the use of two-factor authentication). Two-factor authentication requires something you have (e.g., a token) and something you know (e.g., password).

[6] Class A data is considered highly sensitive personal information that, if compromised, could jeopardize an individual's safety (e.g., names and addresses of children in care). Class A security controls require unique system ID, password requirement, and two-factor authentication.

To monitor the security of the Linkin system, the Ministry receives and reviews reports from Central Services. For example, Central Services provided the Ministry with an annual security report in March 2015. This report provided an overview of security at Central Services' data centre and Ministry-specific risks for the past year. It identified one specific risk related to Linkin. Social Services received a security risk assessment from Central Services on this risk. The Ministry subsequently implemented the changes (e.g., technical and process controls) to mitigate the risk to a level acceptable to the Ministry. The Ministry indicated that it expected to receive another annual security report in the spring of 2016; it has not yet received this report at March 2016.

We assessed whether Linkin and its related IT infrastructure were being properly updated (i.e., patched) to secure it against known vulnerabilities (i.e., system weaknesses). We found that Linkin and its related IT infrastructure were patched on an annual basis, even though critical patch system updates to repair system vulnerabilities were released quarterly. We also found that, as of August 2015, the Linkin database was no longer fully supported by its vendor. This means since August 2015, the Ministry has not received patches to address known security vulnerabilities. The Ministry was not aware that the support had ended for the database that Linkin uses. As shown in **Figure 2**, the Linkin database is one component of the Linkin system. We found all other components of the Linkin system continue to receive support from its vendor.

Being aware of end-of-support dates and updating systems on a timely basis makes systems less susceptible to compromise and failure because vulnerabilities are addressed in a timely manner.

1. **We recommend that the Ministry of Social Services establish a written plan for updating its Linkin system to protect it from known security vulnerabilities.**

4.2 Need to Remove Unneeded Linkin Access Timely

The IT infrastructure (i.e., servers) for Linkin is housed in a data centre operated by a private IT service provider. Confirmed through an independent audit report of the private IT service provider, the data centre is environmentally controlled (e.g., temperature and humidity controls, fire suppression), has an uninterrupted power supply in place, and is physically secure (see **Figure 2**).

Ministry caseworkers, administrative staff, and managers use Linkin. Linkin had over 1,100 users at January 2016–with the majority of users having access to the case management component of Linkin and about 70 users for the financial component.

Linkin had approximately 20 different user roles[7] (e.g., caseworker, admin, supervisor). Specific user roles only have access to the information assigned to that role. Linkin permits only one role per user at a time. Therefore, before assigning a user a new role, the Ministry must remove the previous role.

[7] Roles determine what a user can or cannot do within a system.

The financial component of Linkin includes a payment approval hierarchy. This hierarchy is also user-role driven. In the hierarchy, a user role cannot be vacant if there is another assigned user underneath it. We found the responsibilities assigned to user roles appropriately segregated incompatible functions (e.g., changing payment rates, adding services for payment to care providers).

To access Linkin, one must have a system user account,[8] a password, and a token.

The Ministry used a standard electronic account request form for adding, modifying, or closing Linkin user accounts. The Ministry had made six employees (business approvers) responsible for receiving, reviewing, and approving the account request forms before forwarding them to Central Services for processing. As part of this process, business approvers must assess the assigned role to the user for reasonableness. We tested a sample of 10 account request forms and found all were reviewed and properly approved.

Upon receiving the account request form for a new employee, Central Services established a network account, a Linkin account, and the Linkin application on the employee's computer. Because Linkin requires two-factor authentication, an employee must have a hard token (which is small hardware device). To access Linkin, users must enter a personal identification number (PIN) displayed on the token, followed by their user id and password. New employees receive a token and access once they have completed Linkin training. We tested a sample of new employees with access to Linkin and found that training was provided.

All caseworkers have full access (i.e., access to view and change data) to all children-in-care data in Linkin for child safety purposes. Linkin logs (track electronically) all changes to children-in-care data. We found the Ministry set file restrictions when:

- A case is highly publicized
- A conflict of interest is disclosed by a Ministry staff member

If a caseworker requires access to a restricted file, Linkin provides information as to who to contact to gain such access.

Linkin requires a supervisor to transfer all active case files to another user before closing a user's account (that is, removing unneeded user access). This requirement helps ensure the Ministry always assigns responsibility for case management (i.e., manage services provided to the child in care) to a specific caseworker. Assigning a specific caseworker helps ensure children in care receive services timely.

However, we found the Ministry had not set an expected length of time to close a user's account. For 16 out of 30 users with unneeded access we sampled, they did not have their access removed for over 10 working days after their last day of work with the Ministry. We recognize that the risk of someone inappropriately accessing Linkin is reduced by the need to have a token, which is to be returned upon termination. However, the Ministry did not have evidence that tokens were returned upon termination for all users we tested.

[8] A user often has a user account and is identified to the system by a user name or user id.

We also found the Ministry did not consistently review user access to Linkin. At March 2016, the last time it had reviewed Linkin user access was in December 2013.

Not removing unneeded user access promptly increases the risk that case files are not being managed timely, unauthorized individuals access confidential data, and unauthorized changes are made to data.

2. We recommend that the Ministry of Social Service set out, in a policy, expected timeframes for removing Linkin user access.

4.3 Verification of Caregiver Information Needed and Sufficient Documentation Required for Linkin Payments

In November 2015, as part of its process to put the financial component of Linkin into operation, the Ministry converted certain information (e.g., list of approved foster families) from its previous payment system (FYAP) into Linkin. We found the Ministry had a conversion plan, and checked that it converted the information from FYAP into Linkin accurately and completely.

The Ministry uses Linkin to track key information about the care providers. It needs some of this information (e.g., monthly basic maintenance amount) to initiate payments to care providers related to children in care. It needs other information (e.g., names of individuals living within the foster family household) for case management purposes.

Before the Ministry adds a new provider to Linkin, staff search Linkin to make sure the provider is not already set up in Linkin. If not, staff enter information about the new provider from a paper form. A supervisor reviews and approves the information entered in the Linkin system.

We sampled 10 new providers and found 2 instances where complete information was not entered from the paper form into the Linkin system for care provider families. For example, relatives of the care provider (living in the home with the child) noted on the form were not entered. Inadequate information about individuals in the house could impact the safety of children in care (e.g., individual is restricted from being around a child). The Ministry did not follow its processes, in all cases, to make sure all key case management-related data about care providers is entered into Linkin.

Not having complete information about care providers in which the Ministry has placed children in care could impact the safety of those children.

3. We recommend that the Ministry of Social Services follow its processes to verify the completeness of Linkin case management information entered about care providers of children in care.

Linkin initiates about 4,800 payments each month related to child and family services with about $15 million of payments between November 2015 and January 2016.

The financial component of Linkin connects electronically (interfaces) with MIDAS to pay providers, and record these payments in the Ministry's financial records. The transfer of data between Linkin and MIDAS is encrypted. To protect the confidentiality of information of children in care, MIDAS records only a reference number and does not record children's names.

The Ministry has processes for validating payment data transferred from Linkin to MIDAS and looking for unusual payments. For example, it automatically delays payments for amounts exceeding $10,000 until a Ministry staff member reviews the validity of the amount. Also, it expects staff to review a report, generated each pay run. This report outlines overrides to service rates (e.g., rate set for services like clothing allowance) greater than $1,000 (i.e., payments not in line with usual payment amounts). These processes help identify specific risks associated with the payment process.

The Ministry requires staff to document their review of reports of payments not following usual payment processes. However, we found that staff did not document their review of these reports.

Having staff document the completion of key tasks increases the likelihood of tasks being completed how and when expected. Documentation also enables supervisors to monitor the completion of assigned procedures. Not documenting staff review of reports used to identify unusual payments increases the risk of inappropriate payments.

4. We recommend that the Ministry of Social Services consistently document its review of Linkin reports designed to identify unusual payments.

Upon the Ministry's request, Central Services is responsible for implementing requested changes to Linkin. This includes setting maximum service rates in Linkin. We sampled changes and rates, and found no issues.

The Ministry, along with Central Services, has an established process for identifying, escalating and addressing security incidents related to Linkin. We did not find any security breaches related to Linkin for the 12-month period ended December 31, 2015 (our audit period).

5.0 GLOSSARY

Application – A software program. This includes programs such as web browsers, word processors, spreadsheets, accounting programs, etc.

Database – A software program. A program that interacts with the user, the application, and the database itself to capture and analyze data.

Data Centre – A central location for computer network hardware and software, especially storage devices for data.

Encryption – A method of putting information in code so that only authorized users will be able to see or use the information.

End-of-support date – The date which all forms of services and technical support for a product ceases.

Environmental controls – The controls in place at an organization to manage risks posed by the physical location of computers or network equipment. Examples include fire suppression systems, moisture detectors, and uninterruptable power supplies.

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

Patch – An update to a computer program or system designed to fix a known problem or vulnerability.

Server – A computer that hosts systems or data for use by other computers on a network.

User access controls – The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

6.0 Selected References

Chartered Professional Accountants of Canada (CPA) and the American Institute of Certified Public Accountants (AICPA). (2014). *Trust Services Principles, Criteria, and Illustrations*. Durham: Author.

International Organization for Standardization. (2013). ISO/IEC 27002:2013(E). *Information Technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

Office of the Auditor General of British Columbia. (2010). *Office of the Auditor General of British Columbia, 2009/2010: Report 7, The PARIS System for Community Care Services – Access and Security*. British Columbia: Author.

Provincial Auditor of Saskatchewan. (2015). *Auditor's Report on MIDAS Financial for the 12-month period ended December 31, 2014.* Regina: Author.

The Information Systems Audit and Control Association. (2012). *COBIT 5*. Rolling Meadows: Author.

Western Australian Auditor General. (2014). *Western Australian Auditor General's Report, 2014. Information Systems Audit Report*. Report 14: June 2014. Australia: Author.