Office of the Information and
Privacy Commissioner of Alberta

Investigation Report

Business continuity planning following a system outage

F2013-IR-03/P2013-IR-01/H2013-IR-02

October 24, 2013

Service Alberta
Alberta Treasury Branches
Alberta Health
Alberta Health Services

(Investigations F6336, P2137, H4943 and H4944)

Table of Contents

Introduction

[1] On July 11, 2012, a fire at the Shaw Court building in Calgary caused a service outage (i.e., "the outage"), impacting computer servers that store Albertans' personal and health information. The building housed servers for Service Alberta (SA), Alberta Treasury Branches (ATB), Alberta Health (AH), and Alberta Health Services (AHS) (collectively, the respondents). On July 16, 2012, Alberta's Information and Privacy Commissioner notified the respondents that her Office was investigating the outage.

[2] The Commissioner has received no complaints from individuals regarding their own personal or health information related to the outage. However, each of Alberta's three access to information and privacy laws say the Commissioner is "generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved" and the Commissioner may, "conduct investigations to ensure compliance with any provision of this Act." Therefore, this is a Commissioner-initiated investigation into the respondents' compliance with the *Freedom of Information and Protection of Privacy Act* (FOIP), the *Personal Information Protection Act* (PIPA) and the *Health Information Act* (HIA).

[3] Under her mandate to investigate compliance, the Commissioner established the following purposes for this investigation:

- Examine how personal information stored at Shaw Court is managed by the respondents
- Determine whether current practices and processes are in compliance with FOIP, PIPA and HIA
- Assess any risk to individual privacy resulting from the outage itself or from the interim measures taken until services were restored
- Make recommendations where required

[4] Alberta's three privacy laws require that public bodies, businesses and health custodians take reasonable measures to protect against risks that could affect the confidentiality and integrity of personal and health information. The investigation examined the safeguards that the respondents had in place to protect personal and health information affected by the outage. This includes not only their management of information during this outage, but also their general preparedness for outages.

[5] The investigation found that three of the four respondents had business continuity and disaster recovery plans in place. One of the respondents had components of a business continuity plan in place, but no comprehensive plan. Recommendations on business continuity and disaster recovery planning for all public bodies, organizations and custodians are included in this report.

Background

[6] Shaw Communications Inc. (Shaw) is the building owner and landlord of Shaw Court, located at 6th Street and 3rd Avenue SW in Calgary. The respondents' servers were housed in an IBM Canada data centre, situated on three floors below the 13th floor. On July 11, 2012, one of the electrical breakers in the building failed, which caused a fire in the main transformer room on the 13th floor. In response to the fire, the fire alarm was automatically activated and the main sprinklers immediately engaged, discharging a significant volume of water, damaging equipment and infrastructure on the floors below.

[7] The fire also caused a power outage in the building. When the building power failed, the emergency generators initially engaged, as would be expected. However, the emergency diesel generators also shut down and power was lost throughout the building. As a result, the computer servers in the IBM data centre shut down suddenly in what is known as a "hard stop." This means that systems were not shut down in an orderly manner; rather, power was cut suddenly and systems went offline. In this situation, it is necessary to very carefully re-start systems to ensure no data is lost or corrupted. This is a time-consuming process and it usually means systems are not available during the re-start process.

Scope of this Investigation

[8] The scope of this investigation is limited to whether the respondents had reasonable safeguard measures in place as required under FOIP, HIA and PIPA and whether the confidentiality and integrity of personal or health information was put at risk because of the outage.

[9] Given the relatively short duration of the service interruptions, this investigation did not examine whether the outage affected the respondents' ability to answer individuals' access and correction requests under FOIP, HIA and PIPA, or general freedom of information requests under FOIP. In any case, no one has complained to the Commissioner about the respondents' ability to answer such requests as a result of the outage.

[10] Some systems and services were disrupted for approximately one week, but most critical systems were restored within 48 hours (specific times are provided later in this report). This investigation does not focus on whether systems were restored in a timely manner. Further, this report does not make any comment on whether the respondents made correct decisions regarding the availability requirements of the affected systems. These questions are the purview of other investigating bodies.

Application of Legislation

[11] This investigation focused on the protection of personal information under each of Alberta's three privacy laws. The following section examines the application of FOIP, PIPA and HIA in the context of safeguarding personal information.

Freedom of Information and Protection of Privacy Act

[12] FOIP applies to "personal information" in the custody or control of "public bodies." Service Alberta is a department of the Government of Alberta and, as such, is a public body as defined under section 1(p)(i) of FOIP. I reviewed the listing of systems that were affected by the outage and confirmed with Service Alberta that these systems contained information about identifiable individuals. This information is "personal information," as defined in section 1(n) of FOIP. Therefore, FOIP applies to the information affected by the outage.

[13] The Commissioner's authority to investigate this matter is set out in s. 53(1)(a) of FOIP, which says,

> **General powers of Commissioner**
>
> **53(1)** In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records

Personal Information Protection Act

[14] PIPA applies to "personal information" in the custody or control of "organizations." Alberta Treasury Branches is a corporation and is therefore included in the definition of "organization" under section 1(1)(i) of PIPA. I reviewed the listing of systems that were affected by the outage and confirmed with ATB that these systems contained information about identifiable individuals. This information is "personal information" as defined in section 1(1)(k) of PIPA. Therefore, PIPA applies to the information affected by the outage.[1]

[15] The Commissioner's authority to investigate this matter is set out in s. 36(1)(a) of PIPA, which says,

> **General powers of Commissioner**
>
> **36(1)** In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations to ensure compliance with any provision of this Act;

Health Information Act

[16] The HIA applies to "health information" in the custody or control of "custodians." Alberta Health and Alberta Health Services both fall within the definition of "custodian" in section 1(1)(f) of the HIA. I reviewed the listing of systems that were affected by the outage and confirmed with AH and AHS that these systems contained "registration information" and "diagnostic, treatment and care information" about individuals. This information is "health information," as defined in section 1(1)(k) of the HIA. Therefore, the HIA applies to the information affected by the outage.

[1] Some personal information in the custody or control of ATB may be subject to FOIP; however, this would only apply to personal information found in records that relate to non-arm's length transactions between the Government of Alberta and another party. The personal information in question here is individual banking information, so PIPA applies. See section 4(1)(r) of FOIP and section 2 of the *Personal Information Protection Act Regulation* for further clarification.

[17] The Commissioner's authority to investigate this matter is set out in s. 84(1)(a) of the HIA, which says,

> **General powers of Commissioner**
>
> **84(1)** In addition to the Commissioner's powers and duties under Divisions 1 and 2 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may
>
> (a) at the request of the Minister or otherwise, conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records set out in an enactment of Alberta,

Business continuity planning under Alberta's access and privacy legislation

[18] As outlined above, the personal and health information in question is regulated under Alberta's three privacy laws and the respondents are subject to these laws. All three laws include a duty to protect personal and health information under the respondents' custody or control. The personal and health information protection provisions of FOIP, PIPA and HIA vary in wording, but the intent is similar. Each provision is cited below.

Section 38 of FOIP says,

> **38** The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Section 34 of PIPA says,

> **34** An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Section 60 of HIA says,

> **60(1)** A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
>
> (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,
>
> ...
>
> (c) protect against any reasonably anticipated
>
> (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or
>
> (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,

[19] While the wording is different, there are a number of common elements in the above provisions. Each law says that public bodies, custodians and organizations need to take reasonable measures to protect personal and health information from risks that include unauthorized access and disclosure. Both FOIP and PIPA include a duty to protect against

"unauthorized destruction" of personal information. The HIA says custodians must protect against threats to "integrity" or "loss" of health information.

[20] Taking reasonable measures to protect against risks implies that the respondents need to analyse what kinds of risks may affect personal and health information. In performing this analysis, it is important to consider measures to mitigate these risks. Each law includes the concept of reasonableness,[2] which means that mitigation strategies do not need to be perfect. Information security and breaches may still occur even when reasonable safeguards have been implemented.

[21] Information systems may fail for any number of reasons, which could include fire, water damage and electrical failure, as was the case here. In my opinion, it is reasonable to anticipate that a system may fail for these reasons. The confidentiality of personal and health information held in business systems may be compromised when other systems fail during an outage. For example, physical security alarms may fail, allowing intruders access to computer equipment that stores personal and health information. Further, computer security systems, such as firewalls, authentication services or intrusion detection systems may fail during an outage, compromising an organization's ability to protect personal or health information. Without a plan to respond to a system failure, the confidentiality of personal or health information may be at risk.

[22] In summary, it is reasonable to anticipate information system outages due to fire and other causes. System outages may compromise confidentiality because privacy and security systems may also go offline during an outage. Further, Alberta's three privacy laws make public bodies, organizations and custodians responsible for taking reasonable steps to protect personal and health information against unauthorized destruction, loss and threats to integrity.

Business continuity and disaster recovery planning

[23] Computer system failure caused by a disaster is a reasonably foreseeable risk. To address this risk, organizations establish Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP).

[24] The Information Systems Audit and Control Association's (ISACA) *Glossary of Terms* defines a Business Continuity Plan as, "A plan used by an enterprise to respond to disruption of critical business processes." The same glossary defines a Disaster Recovery Plan as, "A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster."[3]

[25] Based on these two definitions, BCP and DRP may appear to overlap and, in fact, many organizations prepare the two kinds of plans in tandem or may use the two terms interchangeably. A BCP refers to a plan to keep the enterprise functioning, perhaps at a reduced level, during some kind of disaster or service interruption, while a DRP refers to immediate plans to restore systems that are offline because of a disaster. In other words, each type of plan responds to different questions:

[2] While HIA and FOIP both include the concept of reasonableness, it is defined only under PIPA, where section 2 refers to the standard of reasonableness as, "what a reasonable person would consider appropriate in the circumstances."
[3] ISACA Glossary of Terms, http://www.isaca.org/Pages/Glossary.aspx.

Q: Our systems are offline. How do we restore them?
A: Look at the DRP.

Q: Our systems are offline. What do we do until they are restored?
A: Look at the BCP.

[26] The focus of this report is whether the outage put the confidentiality of personal and health information at risk. Lack of either kind of plan or poorly implemented plans could lead to increased risk.

[27] Most BCP and DRP standards our office has reviewed include the following common elements:

1. Establish a planning process with identified teams, resources and executive support.
2. Perform a business impact analysis to identify which systems or business processes are critical to continued operations. This analysis should include consideration of the sensitivity and amount of personal or health information involved.
3. Review the business impact analysis regularly to assess whether priorities need to change to reflect changing requirements.
4. Prepare plans to continue operations and recover from a disaster, based on criticality of systems. Assign priority to more critical systems, which means that critical systems will have faster recovery time objectives and more resources will be spent on recovery.
5. Approve and distribute plans.
6. Train those directly involved in the plan. Make all employees aware of what to do in case of a disaster and what their role may be in ensuring continuous operations. An important component of this is ensuring clear lines of communication are in place and maintained.
7. Test plans regularly.
8. Revise and refine plans, based on test results and changing business requirements.

[28] In short, reasonable business continuity and disaster recovery plans are written, distributed, implemented and tested. If the respondents failed to implement plans that meet these criteria, I will find they have failed in their statutory duties to protect the information in question.

Issues

[29] The respondents are subject to Alberta's privacy legislation. The information in question falls under FOIP, PIPA and HIA and the actions the respondents' took before, during and after the outage relate directly to their duties to protect personal and health information. Therefore, the following four issues for this investigation are:

1. Did Service Alberta make reasonable security arrangements to protect personal information in compliance with section 38 of the *Freedom of Information and Protection of Privacy Act*?

2. Did Alberta Treasury Branches make reasonable security arrangements to protect personal information in compliance with section 34 of the *Personal Information Protection Act*?

3. Did Alberta Health take reasonable steps to protect health information in compliance with section 60 of the *Health Information Act*?

4. Did Alberta Health Services take reasonable steps to protect health information in compliance with section 60 of the *Health Information Act*?

Analysis and Findings

[30] Based on the issues identified above, the analysis and findings of this investigation are presented below for each of the four respondents. In each case I asked the respondents to describe the outage from their perspective, provide information on their plans to prepare for a system outage, describe their immediate response to the outage including any interim measures taken to ensure continued operations, and provide background on service provider roles and relationships.

1. Service Alberta

Did Service Alberta make reasonable security arrangements to protect personal information?

Impact of Outage – Service Alberta

[31] In response to my questions, Service Alberta provided an incident summary and a description of the steps it had taken to prepare for an information systems outage.

[32] Service Alberta runs a consolidated mainframe service for several ministries and government agencies through its Mainframe Application Hosting Services (MAHS). Service Alberta also hosts its own systems on MAHS. According to Service Alberta, the following public bodies and one HIA custodian had a total of 156 applications hosted on MAHS that were affected by the outage:

- Alberta Pensions
- Education
- Justice and Solicitor General
- Seniors
- Service Alberta
- Transportation
- Alberta Health (described in more detail later in this report)
- Energy Resources Conservation Board
- Human Services
- Environment and Sustainable Resource Development

These 156 applications included corporate and individual citizen registries, payroll and cheque issuing systems, student information, licensing and health management systems. The majority of the systems were accessible, online and operational at a backup facility by July 12, 2012. Using a staggered approach, Service Alberta fully recovered all systems to its primary data centre at Shaw Court by 11:15pm on July 16, 2012.

Preparation for an Outage – Service Alberta

[33] Service Alberta provided a copy of its Disaster Recovery Manual for MAHS, dated March 11, 2011.[4] This plan includes a process to declare a disaster, set up a command centre, establishes teams and responsibilities, backup and recovery procedures, implementation plans, testing exercise requirements and disaster recovery plan maintenance. Service Alberta maintains contracts with external service providers for MAHS, which include backup and recovery procedures and testing. Service Alberta reported that it has conducted a disaster recovery testing exercise each year since 2005 and provided a copy of the report from the exercise most recently conducted prior to the outage, in October 2011.

Privacy risk assessment – Service Alberta

[34] Service Alberta reported no data loss as a result of the outage. Service Alberta says its disaster recovery procedures were followed according to plan. Service Alberta and its contractors maintained backup tapes for all data in question. Data was written to the backup tapes in close to real time. Once the systems hosted at Shaw Court went offline, Service Alberta was able to transfer and recover all data after transporting backup tapes to its backup facility in Markham, Ontario.

[35] Service Alberta and many other government systems were offline during the outage. Staff activated contingency measures, as outlined in the MAHS Disaster Recovery Manual and in other written documentation. In some cases, business was interrupted or delayed (for example, motor vehicle registration expiry dates were extended briefly, school transcripts were unavailable, fishing licenses were not required during the outage period, etc.). As stated earlier in this report, whether these delays were acceptable or appropriate does not fall within the scope of this investigation. There is, however, no evidence to suggest these service interruptions or contingency operations compromised the privacy or security of personal information in Service Alberta's custody or control.

[36] Finally, Service Alberta has reported that it has implemented improvements to its disaster recovery stance since this outage. Effective October 2012, all ministries using MAHS now have their data backed up through 'global mirroring,' which means that the backup systems no longer rely on data tapes; rather, data is copied from the MAHS servers to backup servers in real time. Service Alberta now says that in the event of a disaster, MAHS systems will now be recovered within hours, rather than days.

Finding – Service Alberta

[37] As stated previously, a reasonable business continuity plan is written, distributed, implemented, and tested. Because Service Alberta had implemented and tested its business continuity plans, I find that Service Alberta made reasonable arrangements to protect personal information in compliance with section 38 of FOIP. I have no further recommendations for Service Alberta.

[4] In 2010, the Office of the Information and Privacy Commissioner reviewed and accepted a Privacy Impact Assessment from Service Alberta regarding Mainframe Application Hosting Services, which included plans for disaster recovery and physical, technical and administrative security arrangements.

2. Alberta Treasury Branches

Did Alberta Treasury Branches make reasonable security arrangements to protect personal information?

Impact of Outage – Alberta Treasury Branches

[38] ATB reported that the outage affected its computer systems at Shaw Court and disrupted its IT services and infrastructure. This included ATB's internal communications and ATB Online, which meant online services to customers were not available. ATB's systems were down from the afternoon of July 11, 2012, until critical banking systems were restored at approximately 9:00am July 12, 2012. Automated banking machines and point of sale services were available to customers during the outage. As power was restored to the Shaw Court facility, the remainder of ATB's systems and applications were restored by the afternoon of July 13, 2012, in accordance with ATB's Disaster Recovery Plan.

Preparation for an Outage – ATB

[39] ATB provided a copy of its DRP to this office for review. ATB's DRP outlines key roles and responsibilities during a disaster scenario as well as alert and notification requirements for third party vendors and service providers as well as ATB's incident management and response protocols. ATB last tested its DRP for its key lines of business in August 2011. ATB also gave us a listing of its various business units' Business Continuity Plans, showing that all areas had a BCP in place and all had been tested within the previous year.

[40] During the outage, ATB activated its Business Continuity Plans. This meant that employees used pre-established alternative processes to provide banking services to customers. ATB's email service was offline during the outage. Some individuals working directly on incident response were authorized to use personal email accounts, but only to communicate about disaster recovery and systems restoration – no customer personal information was relayed via email. Once systems were restored, ATB's business units reconciled data they had collected through alternative processes (generally on paper forms) with its computer systems. ATB reported that it lost no data as a result of the outage.

Privacy Risk Assessment – ATB

[41] Following the outage, ATB conducted a privacy compliance review looking at the impact of the outage on its key lines of business and business units. Specifically, the review focused on business units that collect, process, disclose and/or store personal information and the associated systems that were affected. As a result of its own investigation, ATB reported that the confidentiality and privacy of personal information was not compromised because of the outage or any contingency measures taken while systems were offline.

Finding – Alberta Treasury Branches

[42] ATB provided evidence to show that it had implemented and regularly tested its business continuity and disaster recovery plans. During and immediately after the outage, ATB executed these plans. Finally, ATB provided evidence that it had reviewed its response to the outage and made recommendations to improve its plans. Therefore, I find that Alberta Treasury Branches

made reasonable arrangements to protect personal information in compliance with section 34 of the *Personal Information Protection Act*. I have no further recommendations for ATB.

3. Alberta Health

Did Alberta Health take reasonable steps to protect health information?

Impact of Outage – Alberta Health

[43] Alberta Health provided an incident summary from their perspective and a description of the steps it had taken to prepare for an information systems outage. We also asked Alberta Health for its business continuity plans.

[44] Alberta Health reported 81 systems were offline during the outage (these are included in the 156 systems mentioned in relation to Service Alberta above). These included directories, registries and systems used to track and manage health system resources and are not used to support direct health care delivery (with one notable exception, described below). According to Alberta Health, the impact of having these systems offline was that some health services providers experienced difficulties completing drug and diagnostic requests, invoice payments to physicians were suspended and some Alberta Health staff were sent home for short periods because of system unavailability. Alberta Health was able to restore all systems by July 15, 2012, at 8:00am.

Preparation for an Outage – Alberta Health

[45] Alberta Health sent a copy of its "IT Disaster Recovery Plan," last revised January 31, 2011. This plan includes a listing of disaster recovery teams and responsibilities, a process for activating the plan, technical recovery procedures, a relocation plan, plan testing requirements and plan maintenance. The document also includes contracts that support the plan, contact lists, a disaster notification process and a plan testing policy that covers various levels of testing from "table-top" exercises (i.e. teams review scenarios through discussion) to full-scale testing (i.e. simulation of a disaster scenario with full deployment of the recovery plan). Testing covers such scenarios as system outages similar to the Shaw Court fire and pandemics, for example.

[46] Alberta Health says its plan is tested annually. Alberta Health provided a report showing that it ran a test of its disaster recovery plan in October of 2011, before the outage. The plan was previously reviewed on January 10, 2012. Alberta Health activated this plan on July 11, 2012, within an hour of its systems going offline.

[47] Alberta Health also sent us a copy of its Incident Management Processes and Resources, last revised April 2011. This document outlines Alberta Health's plans to manage information systems outages at four levels of severity and provide continuing support to users via its service desks. Alberta Health activated this plan following the Shaw Court fire and classified the incident as 'major' because it involved an unplanned outage of mission-critical applications.

[48] Alberta Health keeps daily backups of all databases for 30 days; monthly backups are retained for 12 months; yearly backups are stored for 10 years.

Privacy Risk Assessment – Alberta Health

[49] Alberta Netcare (i.e. Netcare), the provincial electronic health record system, was affected by the outage. Netcare makes summary-level health information available to authorized users throughout Alberta and is used to provide health services. Demographic, prescription and lab report information are included in Netcare[5]. Netcare users access the system from networks secured by Alberta Health Services by logging in with a username and password. When accessing Netcare from outside this secured network (for example, from a physician office or pharmacy), users need to use a device known as a Netcare fob that adds an additional layer of security. The fob generates a number every two minutes that is synchronized with a server housed at Shaw Court. When logging in to Netcare, the user inputs the number generated by the fob, a personal identification number (PIN), plus their username and password. This approach is known as 'two-factor' authentication because users need to have a fob and know their PIN, username and password in order to log in (something you have + something you know = two factors of authentication). The server that manages this two-factor authentication process was offline during the outage.

[50] Alberta Netcare remained online during the outage; however, its authentication system for users outside the AHS-secured network was offline. This meant that Netcare users could access the system from within hospitals, but could not gain access from physician clinics and pharmacies, for example.

[51] Alberta Health weighed the clinical risk of health services providers not being able to access Netcare against the privacy and security risk and decided to relax its authentication process for users outside the AHS-secured network. To maintain access to Netcare during the outage, users were able to log in to Netcare with their username and password only – no Netcare fobs were necessary. The authentication server was restored at 2:46am on July 14, 2012.

[52] I asked Alberta Health officials why the Netcare authentication server had not been identified as a critical system. According to Alberta Health, insufficient resources were assigned to this aspect of business resumption planning and this list was not reviewed until after the Shaw Court fire. This meant that when the Netcare authentication server went offline, there was no plan in place to recover the system quickly. Further, no alternative processes had been contemplated. Unfortunately, Alberta Health was forced to scramble and quickly come up with a work-around in the midst of a crisis.

[53] Alberta Health informed the Commissioner of the Netcare security relaxation at the time and kept our Office briefed on this situation throughout. Alberta Health also committed to conducting an audit of system logs to detect any unusual activity in Netcare following the outage. Alberta Health conducted this audit in August 2012 and reported that it found no anomalies.

Finding – Alberta Health

[54] As stated previously, a reasonable business continuity plan is written, distributed, implemented and tested. Alberta Health had business continuity plans in place prior to the Shaw Court fire.

[5] A more detailed description of Alberta Netcare is available from Alberta Health at www.albertanetcare.ca.

These plans were reviewed and tested regularly. However, Alberta Health had not confirmed its list of critical systems with business areas and established recovery time objectives for these systems due to resource constraints. Because of this, Alberta Health failed to identify an authentication server as being a critical system. An important component of Netcare security infrastructure was offline for 36 hours during the outage. This reduced the strength of Netcare's authentication system, putting Albertans' health information at an elevated risk for this period.

[55] Section 60 of the HIA requires that custodians take "reasonable steps" to protect against threats to the confidentiality of health information. Therefore, the standard of protection under the HIA is one of reasonableness, not perfection.

[56] Alberta Health's plans were reviewed and tested regularly. To find that Alberta Health failed to implement reasonable controls, the investigation would have to reveal that no plans were in place or that the plans were not reviewed or tested. However, Alberta Health presented evidence that they had plans in place for disaster recovery and incident management. This investigation revealed a flaw in Alberta Health's process to review its disaster recovery plans, rather than a failure to implement, review and test plans. Therefore, I find that Alberta Health took reasonable steps to protect health information in compliance with section 60 of the *Health Information Act*.

[57] Alberta Health has since conducted a test of its Disaster Recovery Plan, from January 28-30, 2013, which included testing the Netcare authentication server. Since Alberta Health has corrected the previously noted deficiency in its process to review its plans, I have no further recommendations for Alberta Health.

4. Alberta Health Services

Did Alberta Health Services take reasonable steps to protect health information?

[58] AHS submitted a chronology of the outage and an overview of the affected systems. Our office also received information from AHS on what plans were in place prior to the outage and a detailed Incident Summary Report.

Impact of Outage – Alberta Health Services

[59] The IBM data centre at Shaw Court hosts 689 AHS servers that contain multiple critical networking, clinical and administrative systems, including AHS's internal email and messaging services. In all, a total of 411 medical procedures had to be postponed because of the outage. AHS collected data manually during the outage period. This involved relying on paper patient charts, prescriptions and order entry, for example. Once systems were available AHS took steps to reconcile data to ensure there were no data integrity issues. AHS reported that all critical systems were restored by 7:18am on July 15, 2012. All other systems were restored by 10:05am on July 18, 2012.

Preparation for an Outage – Alberta Health Services

[60] The former Calgary Health Region (CHR) had prepared reports in 2005 and 2008 to identify critical clinical applications. Based on these reports, CHR developed recovery time objectives for

critical systems and developed a series of down-time procedures to allow for manual operation in case critical systems were not available. AHS adopted these plans and also adopted the former CHR's Major Incident Process, which provides instructions on how to coordinate responses to outages and other incidents. AHS provided a copy of its Major Incident Officer Guide, which it followed to respond to the Shaw Court outage. (The Major Incident Process was adopted province-wide following the formation of AHS.) Finally, AHS sent a copy of the Calgary Backup Operational Guidelines. AHS's current Business Continuity Planning policy is included in a Privacy Impact Assessment previously submitted to our Office.

[61] AHS told us that there was no formal Disaster Recovery Plan testing in place for the systems it inherited from CHR, which were housed at Shaw Court. AHS identified this shortcoming before the outage and had a plan in place to address it. The timing of events was, however, unfortunate. AHS had posted a Request for Proposals (RFP) for a Business Continuity Implementation Plan on July 3, 2012, just eight days before the fire on July 11, 2012.

Privacy Risk Assessment – Alberta Health Services

[62] AHS's use of the Shaw Court data centre pre-dates the formation of AHS. Since the formation of AHS, all new critical systems have been implemented with high availability and failover capability and are housed at a different location. AHS says patient confidentiality during the outage was protected through previous privacy and security training provided to staff. Further, AHS reports that all data collected through manual processes during the outage was successfully reconciled to electronic systems as they came back online. Despite the fact AHS was relying on outdated plans from the former Calgary Health Region to respond to the outage, it appears that the confidentiality of health information stored in critical systems at Shaw Court was not compromised.

[63] AHS prepared a comprehensive "Shaw Court Incident Summary Report," which it included in its submission to our office. The Report includes critical observations about AHS's response to the outage and makes several recommendations for improvement. Many AHS business areas noted that staff were not aware of or did not understand downtime procedures. In my view, this is the unfortunate consequence of not having a comprehensive plan in place to prepare for disasters or system outages. As stated earlier, a reasonable business continuity plan is written, distributed, implemented and tested. It appears that parts of a plan were known to key information technology personnel, but not distributed much further. When AHS's internal email and messaging systems failed, many staff did not know what to do and there was no efficient way to communicate downtime procedures. In such situations, employees who are trying to do their best in the face of an outage will take matters into their own hands, as is illustrated below.

Use of personal email and text accounts

[64] The AHS incident report contains a number of references to AHS staff using personal email and text accounts to communicate with each other during the outage period. We asked AHS whether any staff used personal accounts to relay any health or personal information. AHS told us that it had not formally recommended or endorsed the use of personal accounts to continue AHS business. However, they were aware of a number of business units where staff did so. AHS could not confirm whether these communications contained any personal or health information. Any health or personal information sent via email and text accounts would not

have been secured to AHS standards. This represents a risk to privacy which AHS is unable to quantify.

[65] AHS legal counsel communicated a "legal hold" to all staff for records that were created from July 11, 2012, to September 20, 2012, meaning any temporary records created (which would include records created and sent via personal accounts) during and after the outage had to be preserved. The legal hold mitigates the risk that information may be destroyed, but does not mitigate the risk to health and personal information that may remain in personal email and text accounts held on servers outside of AHS's custody or control.

Finding – Alberta Health Services

[66] AHS did not have a comprehensive plan in place to respond to system outages. Instead, AHS relied on plans developed by the former Calgary Health Region. Fortunately, AHS was able to use these plans to restore its systems and reconcile its critical clinical data, confirming no data loss and no data integrity errors. Because AHS had not implemented a comprehensive plan, many of its employees were not familiar with what to do in the face of a critical systems outage. Some AHS staff, having no alternative means to send electronic messages, decided to use personal email and text accounts to conduct AHS business. This represents a risk to privacy as AHS is not able to confirm that no health or personal information was communicated via these channels.

[67] AHS had parts of a plan in place, but the plans were out of date and not widely distributed to its employees. Further, because of this lack of awareness, staff used personal email and text accounts to communicate during the crisis, representing a risk to health and personal information. Therefore, I find that AHS failed to take reasonable steps to protect health information in contravention of section 60 of the *Health Information Act*.

[68] AHS had already taken steps to implement a comprehensive Business Continuity Implementation Plan before the outage through its Request for Proposals from June 2012. I reviewed the RFP and, if fulfilled according to plan, it will mitigate the deficiencies noted in this investigation and in AHS's own Shaw Court Incident Summary Report. As long as AHS implements this plan, I have no further recommendations.

Conclusion

[69] Business continuity and disaster recovery planning is an important component of public bodies', organizations' and custodians' duties to protect personal and health information. As was seen in this report, failure to have these kinds of plans in place or poorly implemented plans can put personal and health information at increased levels of risk. All of the respondents have reviewed their actions following the Shaw Court outage and have taken steps to improve their plans to prepare for similar outages in the future. I would like to thank each of the respondents for their cooperation and openness throughout this investigation.

[70] The Office of the Information and Privacy Commissioner makes the following recommendation to all public bodies, organizations and custodians in Alberta:

Ensure your business continuity plans are written, implemented, distributed and tested and contain the following elements:

1. Establish a planning process with identified teams, resources and executive support.
2. Perform a business impact analysis to identify which systems or business processes are critical to continued operations. This analysis should include consideration of the sensitivity and amount of personal or health information involved.
3. Review the business impact analysis regularly to assess whether priorities need to change to reflect changing requirements.
4. Prepare plans to continue operations and recover from a disaster, based on criticality of systems. Assign priority to more critical systems, which means that critical systems will have faster recovery time objectives and more resources will be spent on recovery.
5. Approve and distribute plans.
6. Train those directly involved in the plan. Make all employees aware of what to do in case of a disaster and what their role may be in ensuring continuous operations. An important component of this is ensuring clear lines of communication are in place and maintained.
7. Test plans regularly.
8. Revise and refine plans, based on test results and changing business requirements.

Investigation Team
Elaine Fitzgibbon, Portfolio Officer
Tara Perverseff, Portfolio Officer
Brian Hamilton, Director, Compliance and Special Investigations