Ottawa

Office of the Auditor General

Audit of Compliance with Legislated Ambulance Service Documentation

Tabled at Audit Committee
April 8, 2019

Table of Contents

Acknowledgements

The team responsible for this audit was comprised of Orbis Risk Consulting Inc. and Suzanne Bertrand and Janet Onyango from the Office of the Auditor General (OAG), under the supervision of Ed Miner, Deputy Auditor General and the direction of Ken Hughes, Auditor General. The team would like to thank those individuals who contributed to this project, and particularly, those who provided insights and comments as part of this audit.

Original signed by:

Auditor General

Executive summary

Introduction

The Audit of Compliance with Legislated Ambulance Service Documentation was included in the 2016 Audit Plan for the Office of the Auditor General (OAG), approved by Council in December 2015.

Background

Since amalgamation in 2001, the City of Ottawa has assumed responsibility for the delivery of paramedic services as defined by the *Ambulance Act* of Ontario. The *Ambulance Act* of Ontario references the requirement to complete documentation in accordance with the *"Ontario Ambulance Documentation Standards"*.

The Ottawa Paramedic Service (OPS) must follow Provincial Ambulance Service Documentation Standards for both Ambulance Call Reports (ACRs) and Incident Reports (IRs). ACRs document whenever ambulance services are provided. Information on a completed ACR can be used for clinical, administrative, research and legal purposes. IRs are used to capture details related to unusual circumstances and events relevant to ambulance services such as circumstances that resulted in harm to a patient or any other person transported in an ambulance or cases of suspicious or unexpected death likely to result in a coroner or police investigation.

The Province conducts re-certification reviews of all ambulance services every three years in addition to ad hoc reviews/inspections. The latest OPS certification review was conducted in April 2016, and it included a detailed review of compliance with Documentation Standards. The City was re-certified. However, the review did find documentation errors on approximately six per cent of the forms tested and made recommendations for improvement.

The OAG chose not to repeat the testing done during this review; rather, we focused on the major changes that have occurred since then. These changes included:

- New Provincial Standards which came into effect April 1, 2017; and
- A new hosted electronic Patient Care Record (ePCR) system that also went live April 1, 2017.

Prior to April 1, 2017, the OPS used a customized commercial ePCR system that resided on City servers. This system was designed to meet the pre-April 1, 2017 Provincial Standards. The new fully hosted ePCR system was competitively procured in 2016 and replaced the previous version. As this new system is critical to the City's ability to comply with the Standards, we reviewed selected aspects of the system.

Audit objectives and scope

The overall objective of this audit was to assess whether the key systems, practices and procedures at the City provide reasonable assurance that the City was complying with Provincial Ambulance Documentation Standards.

Due to the extensive compliance testing done by the Province, the objectives of this audit were to:

- Assess that the hosted ePCR solution provides the functionality and security (i.e. availability, integrity and confidentiality) to completely and accurately process ACRs and IRs to meet Ambulance Documentation Standards; and
- Assess the processes that ensure that ACRs and IRs are compliant with Ambulance Documentation Standards.

The scope of the audit included the following:

- OPS systems and practices related to Ambulance Documentation from April 1, 2017 to completion of audit fieldwork (February 2018); and
- The ePCR system provider's controls, and those of related sub-contractors, which ensure security over City Ambulance Documentation data (OAG testing limited to the extent of access and information contractually available to the City).

Findings

Security monitoring and technical security controls

Given the private and confidential nature of patient records, and the increased security risks associated with moving to a hosted ePCR solution, the audit expected to find practices and controls to mitigate these risks. In reviewing security monitoring and technical controls, we applied audit tests at the following three levels: Device (i.e. the [devices] used in the ambulances), Application (i.e. xxxx, the ePCR system) and Hosting Provider (i.e. xxxx).

The audit identified opportunities to improve security of the ePCR system and data on the [devices].

We found that the security profile of the OPS' [devices] needs to better reflect the risks associated with the ePCR system and the data. In addition to running [the ePCR system], [devices] are configured with additional City-wide applications and functionality. While this additional functionality can serve a variety of practical and appropriate activities, allowing these additional applications also means that the devices are exposed to relatively more security threats compared to a device that is restricted solely to ePCR system functionality. Additionally, we found that the xxxx.

There is an also opportunity to improve security over remote access to [the ePCR system]. xxxx.

We found that neither the City nor [the hosted solution provider] have conducted independent vulnerability assessments or penetration testing on the ePCR system. To validate the effectiveness of security controls and monitoring within the hosted environment, we conducted a series of technical audit tests that replicate potential cyber attacks. xxxx.

The audit identified a risk of a missing [device] not being detected and investigated in a timely manner. OPS has implemented physical security and inventory management controls to track the [devices]. However, OPS does not track the whereabouts of individual [devices] in real time. Additionally, OPS does not conduct a periodic physical inventory reconciliation of [devices].

ePCR system design

There is a risk that paramedics may not complete all the required fields. The ePCR system contains all 141 fields required by the Standards. Some ACR fields were designed to record a specific code to assist in capturing data and improving accuracy. We found that for 11 fields, the ePCR list of available codes is incomplete. Thirty per cent of the required fields are hard coded, completed as a part of the login process or auto-populated (e.g. fields that are time stamped). A further 25 per cent of the fields were designated as mandatory, as such, they cannot be bypassed. However, the remaining 45 per cent of ePCR required fields are neither mandatory, nor hard coded. Having this many fields not required or hard coded can lead to incomplete reports.

We found the OPS manual completed IR forms may not include all of the information required by Provincial Documentation Standards. The OPS completes roughly 6,000

IRs each year, and technical challenges have prevented the integration of an electronic IR form into the current ePCR system. The manual forms completed by paramedics do not include four required fields. Missing these fields could result in staff not fully completing the manual IRs when the nature of the incident is such that they are required.

Monitoring compliance

The audit found the inadequate monitoring of ePCRs to identify where IRs should have been created, and this could place the City at risk of non-compliance with Provincial requirements. OPS is required to audit its ACRs to determine if an IR should have been completed. The OPS has a quality assurance (QA) unit and a process to review a random sample of ePCRs quarterly and assess if all required IRs were submitted. However, this process is retrospective and has a lag time that ranges from a few days to more than three months. In June 2017, the QA unit reported that IRs remained outstanding from its review of ePCRs for the period from April to December 2016.

The Province also requires that service providers such as OPS audit ACRs to determine if they are complete and accurate. These audits are to include recommendations to staff based on the results. The QA unit conducts detailed audits of ePCRs, both at the record level, where individual ACRs are selected and reviewed for specific issues and at the system level, where all records are analyzed to identify issues and anomalies. During 2017, the number of records analyzed decreased significantly. Management indicated that this was the result of shifting of resources and the impact of the implementing [the ePCR system].

ePCR retention

The City's Information Technology Services (ITS) maintained and supported xxxx, the predecessor to the current hosted solution, and continues to do so. OPS indicates that there are approximately 600,000 ACRs in the xxxx database, and they will remain there until migrated to the hosted [the ePCR system] data warehouse. In Phase 2 of [the ePCR system] implementation, [the hosted solution provider] is to map and migrate the xxxx data into [the ePCR system]. Under the contract, [the hosted solution provider] will retain all ePCRs in [the ePCR system] for 10 years, which is longer than the Provincial requirement of five years. While a plan and timeline are being developed to migrate the xxxx records, this work is tracking behind schedule; and there are risks associated with continued delays due to having to maintain the old system.

Conclusion

Overall, OPS has met Provincial Documentation Standards and has maintained its certification status. The migration to a new hosted ePCR platform, [the ePCR system], has gone well to date, but system security and other functionality requires improvement.

OPS should ensure that patient information continues to be safeguarded by xxxx and inventory tracking of the [devices]. Further development and testing of [the hosted solution provider's] online security protocols should be a priority. Additionally, OPS should ensure that the IR form is successfully migrated into [the ePCR system], and the electronic version contains all the required fields.

Recommendations and responses

Recommendation #1

That the City reduce the vulnerability of [devices] to malicious software, data theft as well as unauthorized sharing of data through non-malicious means. This should include revising the existing OPS specific baseline security profile that applies to all of OPS [devices]. xxxx.

Management response:

Management agrees with this recommendation.

The City will revise the existing OPS specific baseline security profile for all OPS [devices]. The timeline for completion is expected to be no later than the end of Q1 2019.

Recommendation #2

That the City, as part of developing an ePCR-specific baseline security profile:

a. xxxx
b. xxxx

Management response:

Management agrees with this recommendation.

The City will work with its ePCR system provider on technical requirements. The timeline for the implementation of an ongoing solution will be determined in consultation with the system provider, but is expected to be no later than the end of Q2 2019. As an interim measure, xxxx.

Recommendation #3

That the City work with its ePCR system provider to confirm and formalize security governance practices and requirements for [redacted]. This may require amending the Service Level Agreement with the ePCR system provider.

Management response:

Management agrees with this recommendation.

The City will engage its ePCR system provider to confirm and formalize security practices. The timeline for completion will be determined in consultation with the system provider, but is expected to be no later than the end of Q1 2019.

Recommendation #4

That the City identify and assess opportunities to engage periodic third-party testing and application security code review of the ePCR system and hosted environment.

Management response:

Management agrees with this recommendation.

The assessment will be completed by the end of Q1 2019.

Recommendation #5

That the City follow up with [the hosted solution provider] so that all required field codes are built into the ePCR system.

Management response:

Management agrees with this recommendation, and it has been implemented.

The City has followed up with [the hosted solution provider] and has confirmed that all required field codes are present within the existing ePCR solution.

Recommendation #6

That the City ensure that, the IR meets the requirements of the Documentation Standards, whether or not an ACR is completed.

Management response:

Management agrees with this recommendation.

The City plans to introduce electronic incident reporting by the end of Q3 2018 with all required fields for the Documentation Standards.

Recommendation #7

That the City review the data security impact on both IRs and ACRs when the IR module is implemented in the ePCR system.

Management response:

Management agrees with this recommendation.

The data security impact will be reviewed as part of the eIR implementation to be completed no later than the end of Q4 2018.

Recommendation #8

That the City implement a regular process of physically counting [devices] to confirm their location, perhaps on a cyclical basis. Further, the costs and benefits of real-time tracking of [devices] through technologies such as Global Positioning System (GPS) or Radio-frequency Identification (RFID) should be considered.

Management response:

Management agrees with this recommendation.

Physical counting of [devices] and tracking through an asset management solution (FDM) is current practice. An RFID trial is currently underway that could also be applicable for real-time tracking of [devices]. The trial period and a review of the cost/benefit of introducing GPS or RFID tracking on devices will be completed by no later than the end of Q3 2019.

Recommendation #9

That the City increase ACR auditing at both the record and the system level.

Management response:

Management agrees with this recommendation.

Management will review the resource requirements needed to increase ACR auditing and how they can be accommodated within existing or future resources by Q4 2018.

Recommendation #10

That the City implement the electronic IR as soon as possible.

Management response:

Management agrees with this recommendation.

The electronic IR platform will be implemented by no later than Q3 2018.

Recommendation #11

That the City establish a procedure to regularly review accesses to all restricted areas and to remove accesses when staff changes occur.

Management response:

Management agrees with this recommendation, and it has been implemented.

A review of access to all restricted areas was undertaken in Q1 2018. A revised procedure has been implemented for the regular review of access on a quarterly basis.

Recommendation #12

That the City finalize and implement the data migration work plan with the hosting service provider as soon as possible. Further, the City should periodically confirm if the 10-year minimum retention period is appropriate in light of legislated requirements.

Management response:

Management agrees with this recommendation.

A transition plan is currently under development with the data transition scheduled to occur prior to the end of Q4 2018. The City will periodically confirm the 10-year retention period in accordance with the legislated requirements.

Detailed audit report

Audit of Compliance with Legislated Ambulance Service Documentation

Introduction

The Audit of Compliance with Legislated Ambulance Service Documentation was included in the 2016 Audit Plan for the Office of the Auditor General (OAG), approved by Council in December 2015.

Background and context

Since amalgamation in 2001, the City of Ottawa assumed responsibility for the delivery of paramedic services as defined by the *Ambulance Act* of Ontario. The *Ambulance Act* of Ontario references the requirement to complete documentation in accordance with the *"Ontario Ambulance Documentation Standards"*. The Province of Ontario funds 50 per cent of land ambulance services and 100 per cent of the cost of the Ottawa Central Ambulance Communications Centre (OCACC).

The Ottawa Paramedic Service (OPS) provides emergency medical coverage across 2,791 square kilometers, while the OCACC provides dispatching services to over 10,000 square kilometers of Eastern Ontario. The OPS serves a base population of approximately 927,000 with a daytime population of approximately 998,000. Approximately 13 per cent of the population is over age 65.[1] The 2018 budget for OPS was $86.5 million with 568 Full Time Equivalents (FTE's) and roughly 90 ambulances and Paramedic Response Units (i.e. PRUs include cars and sport-utility vehicles).

The number of call responses increased from approximately 121,000 in 2012 to 138,000 in 2016 and is expected to grow in line with general population growth and aging. The OPS must follow Provincial Ambulance Service Documentation Standards for both Ambulance Call Reports (ACRs) and Incident Reports (IRs).

[1] Source: 2014 Ottawa Paramedic Service Annual Report

ACRs are an essential medical record used to document whenever ambulance services are provided. Information on a completed ACR can be used for clinical, administrative, research and legal purposes.

IRs are used to capture details related to unusual circumstances and events relevant to ambulance services. For example, they must be completed if there is a complaint about service or if a person is injured while being transported.

The Province conducts re-certification reviews of ambulance services every three years in addition to ad hoc reviews/inspections. The latest OPS certification review was conducted in April 2016, and it included a detailed review of compliance with Documentation Standards. The inspection team, which included a number of experienced paramedics from other Ontario ambulance services, reviewed approximately 300 records. The City was re-certified. However, the review did find documentation errors of approximately six per cent of the sample tested and made recommendations for improvement. In addition, the Province conducted an ad hoc, smaller scope review in August 2016. The OAG confirmed with Provincial officials that they plan to continue these reviews.

The OAG did not repeat the testing done during these reviews; rather, we focused our work on the major changes that have occurred since then. These changes included:

- New *Ontario Ambulance Documentation Standards* which came into effect April 1, 2017; and
- A new hosted electronic Patient Care Record (ePCR) system that also went live April 1, 2017.

Prior to April 1, 2017, the OPS used a customized commercial off-the-shelf ePCR system. The system was hosted on City servers with data collected primarily on tablets in each of the City's ambulances and Paramedic Response Units (PRUs). This system was designed to meet the pre-April 1, 2017 Provincial Standards.

The new fully hosted ePCR system was competitively procured in 2016 and replaced the previous version. In addition to the system being hosted by a subcontractor of the vendor, there were other changes to the application to make it compliant with the new Standards. The change in the vendor relationship to a hosted solution is significant. The OPS is less reliant on the City's Information Technology Services (ITS) and accepts more responsibility to manage its relationship with the vendor.

As this new system is critical to the City's ability to comply with the Standards, selected aspects of the system were reviewed as part of the audit.

Audit objectives and scope

The overall objective of this audit was to assess whether the key systems, practices and procedures at the City provide reasonable assurance that the City was complying with Provincial Ambulance Documentation Standards.

Audit objectives

Due primarily to the extensive compliance testing of Ambulance Documentation undertaken during the triennial Provincial certification process, the objectives of this audit were to:

- Assess that the hosted ePCR solution provides the functionality and security (i.e. availability, integrity and confidentiality) to completely and accurately process ACRs and IRs to meet Ambulance Documentation Standards; and
- Assess the processes that ensure that ACRs and IRs are compliant with Ambulance Documentation Standards.

For each of these objectives, criteria (listed in Appendix A) were developed from material gathered from planning interviews, document review and research. The source(s) for the criterion included: Ontario Ambulance Documentation Standards, Ambulance Call Report Completion Manual, Provincial Certification Team Checklist, Enterprise Risk Management Policy and Information Security Policy, as applicable.

Scope

The scope of the audit included the following:

- OPS systems and practices related to Ambulance Documentation from April 1, 2017 to completion of audit fieldwork (February 2018); and
- The ePCR system provider's controls, and those of related sub-contractors, which ensure security over City Ambulance Documentation data (OAG testing limited by the extent of access and information contractually available to the City).

The scope of the audit did not include the following:

- Dispatching services provided through the OCACC;
- A detailed review of compliance of individual ACRs as these were assessed as part of the Provincial re-certification review; and
- The competitive procurement of the new ePCR system.

Audit approach and methodology

The audit methodology included the following activities:

- Interviews and process walkthroughs with staff members involved in monitoring compliance with Ambulance Documentation Standards and those involved in managing the ePCR system contract;
- Review of relevant documentation (e.g. OPS organizational charts, training documents, Provincial legislation, quality standards, by-laws, policies, procedures, contracts and reports);
- Testing the ePCR system security controls, including:
  - Security controls associated with the [devices] used in the ambulances;
  - Security controls associated with the vendor's application;
  - Security controls within the hosted environment;
  - Plans and processes to ensure ePCRs are maintained and available for five years as required by the Ambulance Documentation Standards; and
- Other audit techniques including the review and analysis of reports and examples of supporting documentation.

The audit fieldwork was conducted from October 2017 to February 2018.

Audit observations and recommendations

Audit objective #1

Assess that the hosted ePCR solution provides the functionality and security (i.e. availability, integrity and confidentiality) to completely and accurately process ACRs and IRs to meet Ambulance Documentation Standards.

To assess this objective, we examined the following four areas:

- Security monitoring and technical security controls;
- ePCR required fields;
- IR module in ePCR system; and
- Theft or loss of mobile devices.

1.1 Security monitoring and technical security controls

Given the private and confidential nature of patient records and the increased security risks associated with moving to a hosted ePCR solution, the audit expected to find highly effective practices and controls to sufficiently mitigate these risks. These security risks may include unauthorized access, and loss, theft or corruption of patient information. Mitigation of these risks requires effective practices and controls to prevent, detect and manage security incidents. Overall responsibility for the security of patient records lies with the OPS Chief. The related practices and controls are shared among OPS, the City's Information Technology Services and the third-party hosting service provider (xxxx or [the hosted solution provider]).

In reviewing security monitoring and technical controls, we applied audit tests at the following three levels:

- Device (i.e. xxxx) Level – [devices] are "rugged" tablet devices that are designed to withstand a physically demanding environment. They are used in the ambulances and other OPS vehicles to enable the input, storage and transmission of patient information.
- Application (i.e. [the ePCR system]) Level – [the ePCR system] is the ePCR system that resides on [devices] and centrally with [the hosted solution provider]. [The ePCR system] can also be accessed via the Internet.
- Hosting Provider – [the ePCR system] is hosted by [the hosted solution provider]. Among their responsibilities as host, [the hosted solution provider] is expected to support the prevention, detection and management of incidents that threaten the security of information entered into [the ePCR system].

[Device] security

The audit identified several examples of effective operating procedures and mechanisms that improve security of the ePCR system and data on the [devices]. These include effective processes for limiting access to authorized users and encrypting

patient information. In addition, [devices] reflect the current suite of security controls applicable to any City-owned device (e.g. up-to-date antivirus software, restricted administrative privileges, etc.). However, we did identify some weaknesses and exposures to security risk that require attention.

In addition to running the [ePCR system], [devices] are configured with additional applications and functionality. Consistent with City standards for laptops, the [device] configuration provides users with a Windows Desktop and access to a range of standard functionality including Internet browsing capability and access to applications such as Microsoft Office and Google Earth. While this additional functionality can serve a variety of practical and appropriate activities, allowing these additional applications also means that the devices are exposed to relatively more security threats compared to a device that is restricted solely to ePCR system functionality. xxxx.

The audit testing also found that xxxx.

The weaknesses and exposures identified through the testing of [devices] are not unique to these devices or the OPS environment. They are consistent with observations included in another audit conducted by the Office of the Auditor General[2] on security related to mobile devices used across the City. What is unique about OPS' [devices], is the highly private and confidential nature of ePCRs that are entered, stored and transmitted via these devices. Therefore, we believe that the security profile of the OPS' [devices] needs to better reflect the risks associated with protecting the ePCR system and data.

Recommendation #1

> That the City reduce the vulnerability of [devices] to malicious software, data theft as well as unauthorized sharing of data through non-malicious means. This should include revising the existing OPS specific baseline security profile that applies to all of OPS [devices]. xxxx.

Management response:

> Management agrees with this recommendation.
>
> The City will revise the existing OPS specific baseline security profile for all OPS [devices]. The timeline for completion is expected to be no later than the end of Q1 2019.

[2] See the Audit of Information Technology (IT) Remote Access (2017)

Application (i.e. [the ePCR system]) security

The audit found that [the ePCR system] application has a number of effective security features and attributes. These include the existence of an automated process to ensure the application is updated with the latest patches on a timely basis. The audit also noted that there is a requirement that users provide a unique name and password to access the application through a [device] or remotely via the Internet (i.e. using xxxx). We also found that the majority of potentially risky application functionality had been disabled or removed. Finally, access to the application was found to be appropriately restricted based on the individual user's approved role.

There is an opportunity to improve remote access to [the ePCR system]. At the time of testing, xxxx.

Recommendation #2

That the City, as part of developing an ePCR-specific baseline security profile:

a. xxxx
b. xxxx

Management response:

Management agrees with this recommendation.

The City will work with its ePCR system provider on technical requirements. The timeline for the implementation of an ongoing solution will be determined in consultation with the system provider, but is expected to be no later than the end of Q2 2019. As an interim measure, xxxx.

Hosting provider (i.e.) security

As noted earlier, there is a potential for increased risk when moving from an in-house solution (xxxx), where the City has direct responsibility and visibility to a hosted solution ([the ePCR system]) where a third party is entrusted to support the security of the ePCR system. The audit expected that as the hosting provider, [the hosted solution provider] would have formal and effective capabilities to xxxx.

Our interviews and document review found a number of appropriate features and processes. These included a business impact assessment and threat/risk assessment conducted by ITS on the hosted solution. ITS also validated that [the hosted solution provider's] baseline security met the requirements that were set out in the City's

Request for Proposal. We also found that the hosted environment featured appropriate network security controls, including the firewalls and proxies, as well as the capability to monitor for security incidents at the application, network and operating system level.

To validate the effectiveness of security controls and monitoring within the hosted environment, we conducted a series of technical audit tests. xxxx.

xxxx. These activities help identify actions and responses needed to address ever-evolving cyber threats. The OAG believes that it is worthwhile to carry out such activities on a periodic basis given the potential impact of unauthorized access to this ePCR system and the City's records.

Recommendation #3

That the City work with its ePCR system provider to confirm and formalize security governance practices and requirements for xxxx. This may require amending the Service Level Agreement with the ePCR system provider.

Management response:

Management agrees with this recommendation.

The City will engage its ePCR system provider to confirm and formalize security practices. The timeline for completion will be determined in consultation with the system provider, but is expected to be no later than the end of Q1 2019.

Recommendation #4

That the City identify and assess opportunities to engage periodic third-party testing and application security code review of the ePCR system and hosted environment.

Management response:

Management agrees with this recommendation.

The assessment will be completed by the end of Q1 2019.

1.2 ePCR required fields

Electronic Patient Care Record (ePCR) – ACR

The audit expected to find that the ePCR system reflects the latest version of the ACR and contains all the information required by the April 2017 Ambulance Documentation Standards (the Standards). Completed ePCRs represent essential medical records

documenting circumstances and events relevant to the proper provision of ambulance services. The audit found that the ePCR system contains all 141 fields required by the Standards. There are 23 fields with minor differences, such as where a date field and time field are merged into one field, but the differences do not impact the ability of the ePCR system to capture the required information.

Some ACR fields were designed to record a specific code to assist in capturing data and improving accuracy. We found that for 11 fields, the ePCR list of available codes was incomplete. Examples of missing field codes included mechanism of injury fields and others that relate to groups of fields. We notified OPS management of the missing field codes who in turn followed up with [the hosted solution provider]. As of the conclusion of our fieldwork, the issue has yet to be resolved. OPS management indicate that they will continue to follow up with [the hosted solution provider].

OPS management has also been in discussions with the Province regarding fields with minor differences and has advised [the hosted solution provider].

Mandatory fields

The Standards require paramedics to complete all fields applicable for the call. For operational reasons, OPS has not configured the ePCR system to make all fields mandatory such that they cannot be bypassed. OPS' objective is to provide its paramedics with the tools that they need to be compliant. Roughly one quarter of the 141 ePCR fields are configured as mandatory in the system. An additional 43 fields are hard coded, completed by the paramedic as part of the login process or auto-populated (e.g. fields that are time stamped).

The OAG is not recommending that more fields be made mandatory. However, as 45 per cent of ePCR fields are neither mandatory nor auto-populated, there is a risk that paramedics may not complete all the required fields. This increases the importance of monitoring completed forms, discussed in section 2.1 below.

Recommendation #5

> That the City follow up with [the hosted solution provider] so that all required field codes are built into the ePCR system.

Management response:

> Management agrees with this recommendation, and it has been implemented.

> The City has followed up with [the hosted solution provider] and has confirmed that all required field codes are present within the existing ePCR solution.

Incident reports (IRs)

Implementation of IRs in the ePCR system

The audit expected to find that the ePCR system reflected the latest version of the IR and that it contained all the information required by the Standards. However, the audit found that the ePCR solution currently does not include electronic IRs; and as a result, IRs continue to be completed manually.

The OPS completes roughly 6,000 IRs each year. Originally, the new hosted ePCR solution was scheduled to include the implementation of an electronic IR by Q1 2018. Management has indicated that technical challenges with integration that were known early in the project prevented this from happening so a decision was taken to defer implementation. Management indicates that as of May 2018 implementation of the IR solution is imminent.

The importance of implementing the electronic IR is further discussed below in Section 2.1.

Manually completed IR forms

The OPS manual IR form has fields to collect most, but not all of the information required by the Standards. The form is missing four fields, as follows:

- Three relate to damaged/malfunctioning equipment. Management indicated these fields are captured on the separate Damaged/Malfunctioning Equipment Form. However, the Documentation Standards require that the IR include these fields.
- One relates to the “dispatch and priority code”.

Missing these fields could result in staff not fully completing the manual IRs when the nature of the incident is such that these fields are required. The IR form also does not include instructions to attach a copy of the applicable ACR, which is also required by the Standards.

OPS indicated that when documenting incidents involving damaged/malfunctioning equipment, a Damaged/Malfunctioning Equipment Form (DMEF) could substitute for an IR. Although the stand-alone DMEF has the required IR fields for a call if an ACR is completed, the DMEF does not have all the required fields in cases where no ACR form is completed. Our view is that recording these incidents outside of the regular IR

process increases the risk of incomplete or missing reports. Monitoring of completed IRs is discussed below in Section 2.1.

Recommendation #6

That the City ensure that, the IR meets the requirements of the Documentation Standards, whether or not an ACR is completed.

Management response:

Management agrees with this recommendation.

The City plans to introduce electronic incident reporting by the end of Q3 2018 with all required fields for the Documentation Standards.

1.3 IR module in ePCR system

The IR module proposed by the ePCR solution vendor is a product from another software vendor. Due to the possible risks involved in integrating two systems into one solution, the audit planned to confirm that the IR module did not cause data security issues for IRs or for ACRs. However, as mentioned above in section 1.2, the IR module has not been implemented; and therefore, no testing was possible.

Recommendation #7

That the City review the data security impact on both IRs and ACRs when the IR module is implemented in the ePCR system.

Management response:

Management agrees with this recommendation.

The data security impact will be reviewed as part of the eIR implementation to be completed no later than the end of Q4 2018.

1.4 Theft or loss of mobile devices

The audit expected to find security measures, procedures and mechanisms to protect ePCR information that may be resident on mobile devices (i.e. [devices] or encrypted USB keys). This is to address situations where a [device] or encrypted USB key is lost or otherwise accessed by an unauthorized user with both the motivation and sophisticated skills to extract ePCR from the device. As noted above, an ePCR resident on a [device] is protected by encryption and multiple access controls. Moreover, there are xxxx.

We also found that OPS has implemented physical security and inventory management controls and practices to track the [devices]. These controls are supported by physical security measures, formal practices for handling [devices], real-time record keeping and appropriate segregation of potentially incompatible responsibilities. OPS uses File Data Management (FDM) software to track its 300 [devices]. This software is integrated with scanning technology to track the location and status of each [device]. In addition to inventory tracking, FDM is used to ensure that every [device] in circulation undergoes preventative maintenance at least once every 60 days.

Notwithstanding the existence of various physical and management controls, the audit identified a number of conditions that increase the likelihood of a missing mobile device not being detected and investigated in a timely manner. These risks relate to the fact that (1) there is currently no capability to confirm the real-time whereabouts of an individual [device]; (2) OPS does not conduct a periodic physical inventory reconciliation of [devices]; and (3) it is the responsibility of the person assigned with the device to report it as lost or stolen. Under these conditions, it is possible for a [device] to be missing or lost for up to 60 days (i.e. when it would be flagged for periodic maintenance) before being detected.

Recommendation #8

> That the City implement a regular process of physically counting [devices] to confirm their location, perhaps on a cyclical basis. Further, the costs and benefits of real-time tracking of [devices] through technologies such as Global Positioning System (GPS) or Radio-frequency Identification (RFID) should be considered.

Management response:

> Management agrees with this recommendation.
>
> Physical counting of [devices] and tracking through an asset management solution (FDM) is current practice. An RFID trial is currently underway that could also be applicable for real-time tracking of [devices]. The trial period and a review of the cost/benefit of introducing GPS or RFID tracking on devices will be completed by no later than the end of Q3 2019.

Audit objective #2

Assess the processes that ensure that ACRs and IRs are compliant with Ambulance Documentation Standards.

To assess this objective, we examined the following two areas:

- Compliance monitoring; and
- Retention of PCRs.

2.1 Compliance monitoring

The audit expected to find that OPS management monitors its ACRs and IRs for compliance with Documentation Standards. The Provincial Certification Checklist lists the minimum requirements for monitoring and audit of documentation by the service provider. This includes the Ambulance Act, which requires that the service provider have a quality assurance program to ensure compliance with legislated requirements. For Documentation Standards, the requirements include that:

- ACRs are completed where required;
- ACRs are accurate;
- ACRs are timely;
- IRs are completed where required;
- IRs are accurate; and
- IRs are timely.

The audit found that there are monitoring processes in place as OPS has an active quality assurance (QA) program lead by its QA unit. The Commander of the QA unit advises the Program Manager, Operational Support on compliance rates. The Program Manager in turn verbally updates the Paramedics Chief on key QA results such as IR and [the ePCR system] reporting. However, there are areas that require improvement as detailed below.

ACRs completed where required

An ACR is required for each request for ambulance service where the paramedic arrives on the scene. This includes where there is no contact with the individual for whom the request was made.

Unique ACR numbers are generated by the Provincial dispatcher and verbally passed on to OPS paramedics who manually enter them into the ePCR system. Ideally, to ensure ACRs are completed where required, OPS would match the ACR numbers in the Provincial dispatch system to those in the ePCR system. However, for the period from May to October 2017, from 8 to 14 per cent of the ACR numbers did not match.

These differences prevent OPS from being able to rely on this matching to ensure completeness.

As an interim solution, superintendents are performing shift envelope audits. Superintendents select a sample of one to four crew shifts each day. They compare the dispatch data to the ePCRs to confirm that the crew completed all necessary ePCRs. The results are documented in the shift audit log and duty log. As its long-term solution, OPS plans to have the call number auto-populated in the ePCR from the dispatch system.

ACRs accurate

The Province requires that service providers audit ACRs to determine if they are complete and accurate and to make recommendations to staff after auditing them. The QA unit conducts detailed audits of ePCRs, both at the record level, where individual ACRs are selected and reviewed for specific issues and at the system level, where all records are analyzed to identify issues and anomalies.

At the record level, the number of records audited was significantly lower in 2017 than in 2016. Management explained that this was a result of shifting resources to other priorities including supporting the ePCR implementation and other service priorities such as Canada 150 events.

At the system level, OPS uses Business Intelligence software to analyse all ePCRs. In 2017, however, there was a delay in building the underlying reporting tables used by the new version of the Business Intelligence software. As such, there was no system level monitoring of [the ePCR system] data from implementation in April until October 2017. To compensate for the lack of system-level monitoring, the QA unit checked a sample of specific fields. The results for one of the two checked fields found a 68 per cent compliance rate. This is well below the 90 per cent rate required for the Provincial re-certification. OPS plan to share these results with its paramedics and superintendents and to continue monitoring.

Recommendation #9

That the City increase ACR auditing at both the record and the system level.

Management response:

Management agrees with this recommendation.

Management will review the resource requirements needed to increase ACR auditing and how they can be accommodated within existing or future resources by Q4 2018.

ACRs timely

The Standards require that paramedics complete ACRs as soon as possible following the event and prior to the end of the scheduled shift or work assignment during which the documented event occurred. The 2017-2018 OPS Internal Clinical Documentation Audit Program states that the QA unit is to audit all non-finalized ePCRs each week.

We found that these audits were not done for most of 2017 due to a [the ePCR system] system problem. OPS management indicated that the problem was “90 per cent resolved” as of November 2017 and reinstated reporting to OPS operational managers. We confirmed that the number of non-finalized ePCRs began decreasing once the system problem was resolved, and we expect OPS management to continue monitoring non-finalized ePCRs.

IRs completed where required

City policy states that superintendents are responsible for monitoring and ensuring IRs are completed and submitted as soon as possible after an incident, usually before the end of the shift where the incident occurred. The City is also required to audit its ACRs to determine if an IR should have been completed. The QA unit has a process to review a random sample of ePCRs each quarter and assess if all required IRs were submitted. We found that the review process was completed for the first quarter of 2017, but it was not done for the second quarter after the new Documentation Standards and the implementation of [the ePCR system]. In December 2017, management indicated they were trying to catch up on Q2 and Q3 IR audits.

The QA unit’s process is completed retrospectively with a lag time that ranges from a few days to more than three months. QA follows up with paramedics and their supervisor on missing documentation or information identified from the quarterly monitoring process to confirm that the required IRs have been created. However, there can be additional delays after QA has reported. In June 2017, the QA unit reported that

IRs remained outstanding from its review of ePCRs for the period from April to December 2016.

As discussed above in section 1.2, the implementation of the electronic IR continues to be delayed. Once implemented, we would expect completion rates for IRs to improve as key words in the ePCR will automatically trigger the generation of an IR. The electronic IR is also expected to improve compliance monitoring.

The inadequate monitoring of ePCRs to identify where IRs should be created could place the City at risk of non-compliance with Provincial requirements. This increases the importance of moving forward with the electronic IR.

Recommendation #10

That the City implement the electronic IR as soon as possible.

Management response:

Management agrees with this recommendation.

The electronic IR platform will be implemented by no later than Q3 2018.

IRs accurate and timely

Service providers are required to audit all IRs for accuracy and completeness; to make recommendations to staff after auditing the IRs; and to address recommendations resulting from an IR audit to mitigate reoccurrence. We found that QA staff read, triage and log every IR received and escalate to OPS management as required. The process of monitoring ACRs to identify situations where an IR should have been completed is discussed above.

2.2 Retention of PCRs

As per legislated requirements, OPS must retain patient records for a minimum of five years. In addition to the legal requirements, maintaining and accessing these records allows OPS to fulfill requests from authorized third parties such as the patient, a coroner or law enforcement. Completed records are also used internally within OPS. Access to these records is limited to the OPS Professional Practices Unit (PPU).

Security of completed paper forms

The *Ambulance Act* and the *Personal Health Protection Act* require that reports be secured from unauthorized access as they contain information that could identify a

patient. OPS stores hard copy manual documentation related to completed ACRs and IRs in a file room with controlled card reader access. There is dual authentication as both card reader access and a personal identification number are required.

With staff changes over time, the employees that require access to the file room also changes. We found that OPS management had not reviewed which individuals had card reader access to the file room in order to ensure access was limited to authorized staff. In connection with this audit, OPS management reviewed file room access and reduced it from 45 to 31 individuals. OPS management indicate they will review the access list quarterly going forward.

Recommendation #11

> That the City establish a procedure to regularly review accesses to all restricted areas and to remove accesses when staff changes occur.

Management response:

> Management agrees with this recommendation, and it has been implemented.
>
> A review of access to all restricted areas was undertaken in Q1 2018. A revised procedure has been implemented for the regular review of access on a quarterly basis.

Retention of ePCRs

Prior to the implementation of the [the ePCR system] hosted solution in Q2 of 2017, ITS was responsible for maintaining the xxxx database and providing relevant support. OPS indicates that there are approximately 600,000 ACRs in the xxxx database. These records relate to calls prior to transitioning to the hosted [the ePCR system] environment. OPS' plan is to migrate these records from xxxx to [the ePCR system] where they will be retained.

As part of the contract, [the hosted solution provider] is responsible to ensure the retention of the ePCRs for 10 years. Under Phase 2 of the [the ePCR system] implementation plan, [the hosted solution provider] is responsible to map and migrate the xxxx data held by ITS to the hosted [the ePCR system] data warehouse. While the Phase 2 work plan is not expected to be approved until the end of Q2 2018, discussions on migration with [the hosted solution provider] and ITS began in 2017. Interviews with OPS indicated that [the hosted solution provider] completed the mapping of OPS' xxxx records to [the ePCR system] in December 2017.

While there is evidence that a plan and timeline are being developed for the migration of xxxx records, this work is tracking behind original expectations; and there are risks associated with continued delays. Not only does the existence of two databases create additional complexity for PPU as they routinely retrieve records from both sources, there may be additional risks associated with storing xxxx data on a legacy server maintained by ITS. While investigating the details of the xxxx legacy system was beyond the scope of this audit, there is often a greater risk of system failure, data corruption or data loss when there is reliance on legacy systems.

Recommendation #12

That the City finalize and implement the data migration work plan with the hosting service provider as soon as possible. Further, the City should periodically confirm if the 10-year minimum retention period is appropriate in light of legislated requirements.

Management response:

Management agrees with this recommendation.

A transition plan is currently under development with the data transition scheduled to occur prior to the end of Q4 2018. The City will periodically confirm the 10-year retention period in accordance with the legislated requirements.

Appendix A – Audit objectives and criteria

Overview of the audit objectives and criteria

Audit objective #1: Assess that the hosted ePCR solution provides the functionality and security (i.e. availability, integrity and confidentiality) to completely and accurately process Ambulance Call Reports (ACRs) and Incident Reports (IRs) to meet Ambulance Documentation Standards.	
1.1	Criteria 1: ePCR is secure, providing availability, integrity and confidentiality.
1.2	Criteria 2: ePCR reflects latest version of ACR and IR and contains all information required by Standards.
1.3	Criteria 3: IR module secure and does not cause data security issues in ePCR system for ACR and IR.
1.4	Criteria 4: Theft or loss of mobile equipment will not result in release of patient information.
Audit objective #2: Assess the processes that ensure that ACRs and IRs are compliant with Ambulance Documentation Standards.	
2.1	Criteria 1: Management adequately monitors compliance with Documentation Standards.
2.2	Criteria 2: Records are available for a minimum period of five years from documented event.