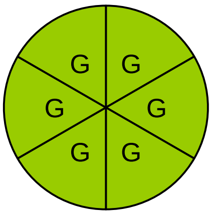
Internal Audit

IT Application Review

March 2017

Report Assessment



This report has been prepared solely for internal use as part of NHS Lothian's internal audit service. No part of this report should be made available, quoted or copied to any external party without Internal Audit's prior consent.

Contents

Introduction

NHS Lothian relies on IT systems to ensure the safe and effective delivery of care. As part of our strategic planning exercise, internal audit agreed to conduct an annual review of controls over key IT systems. In 2016-17, the review considered the links between primary and secondary care IT systems.

NHS Lothian, and associated GP practices rely on national systems. All GP practices use a Document Management application called Docman. Two clinical systems are used in Primary Care: Vision and EMIS.

Key IT application interactions between primary and secondary care are:

Information flows from primary care (Vision and EMIS) to secondary care systems

- National software called SCI Gateway is used in primary care to make electronic referrals to secondary care
- The GP Order Communications system, ICE, is used to request laboratory tests and send clinical details from GP practices to the laboratory software
- National software that extracts relevant data from patient records in Vision/EMIS. These include the Emergency Care Summary (ECS), Key Information Summary (KIS) and electronic Palliative Care Summary (ePCS)
- Software called SCI Diabetes is also used by Diabetes specialists in secondary care. This SCI diabetes software is auto-populated with data including smoking status and blood pressure from Vision and EMIS.

Information flows from Secondary Care to Primary Care systems

- Electronic Document Transfer (EDT) system is used to send data from secondary care systems, including TRAK, Radiology, iLabs and screening reports, to primary care systems
- Information from TRAK, Laboratories and Radiology system is also sent to the SCI store system. This SCI store system can be consulted by clinicians in primary care
- Primary care can consult the SCI diabetes system via username and password.

Scope

The objective of the audit was to evaluate key controls over links between primary and secondary care IT systems.

The audit considered the extent to which controls provide reasonable assurance that:

- Data transferring between primary and secondary care systems is complete and accurate
- Duplicate data transfers are not processed by the target system

- Rejected data transfers are monitored and fixed on a timely basis

- Data is transferred between primary and secondary care systems via encrypted and/or secure channels

- Logical access to interface functionality between primary care and secondary care systems is restricted to appropriate personnel

- Adequate electronic authorisation is provided for data transfers should it be required

  NB This internal audit did not assess the controls around security access management and authentication for the different systems in scope. These controls were not included in the scope of this internal audit recognising the internal audit days available.

Acknowledgements

We would like to thank all staff consulted during this review, for their assistance and cooperation.

Executive Summary

Conclusion

The processes and key controls in operation over links between primary and secondary care IT systems are for the most part operating effectively. Opportunities for improvement were identified regarding the absence of automated alerts to report data transfer errors between ECS and Vision / EMIS. We also noted that there was no service level agreement for the resolution of TRAKcare documents that are rejected by EDT.

Additionally, we noted the absence of encryption for the communication between a number of systems and the sharing of a generic and privileged account to monitor a system interface.

Summary of Findings

The table below summarises our assessment of the adequacy and effectiveness of the controls in place to meet each of the objectives agreed for this audit. Definitions of the ratings applied to each action are set out in Appendix 1.

No.	Control Objective	Control objective assessment	Number of actions by action rating			
			Critical	Significant	Important	Minor
1	Data transferring between primary and secondary care systems is complete and accurate.	Green	-	-	2	-
2	Duplicate data transfers are not processed by the target system.	Green	-	-	-	-
3	Rejected data transfers are monitored and fixed on a timely basis.	Green	-	-	-	-
4	Data is transferred between primary and secondary care systems via encrypted and/or secure channels.	Green	-	-	1	-
5	Logical access to interface functionality between primary care and secondary care systems is restricted to appropriate personnel.	Green	-	-	1	-
6	Adequate electronic authorisation is provided for data	Green	-	-	-	-

	transfers should it be required.	🟩				

As part of this review, we asked National Services Scotland (NSS) staff for evidence regarding the operation of some key controls over data transfers to the ECS system. This evidence had not been received at the point of producing this report. As such, we have been unable to validate these key controls. Additional findings may be raised once this evidence has been examined. These key controls are detailed as follows:

- Data transfers between Vision/EMIS via eLinks to Emergency Care Summary (ECS) are encrypted via HTTPS.
- Access to monitor the interface between Vision/EMIS and ECS is restricted to the NSS Service Desk team.

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention (60 points and above).
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points).
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less).

Main Findings

We noted a number of areas of good practice during the review.

- Duplicate documents sent from iLab and TRAKcare to EDT are rejected.

- We validated for a sample of mandatory fields in the ICE and SCI Gateway systems, that they do not allow a user to submit a secondary care referral unless these fields have been completed.

We identified four important issues during the review:

- There is no formal service level agreement for the resolution of TRAKcare documents that are rejected by EDT.

- There are no automated controls within the ECS system to validate the accuracy and completeness of patient records extracted from the Vision/EMIS systems. It should be noted that the ECS system admin team, which monitors ECS, is part of National Services Scotland (NSS).

- Data transfers between the TRAKcare and EDT systems are not encrypted.

- A generic and privileged user account is shared by several teams to monitor the interface between SCI Gateway and TRAKcare.

Further details of each of these points are set out in the Management Action Plan, at page six of this report.

The following terms are used in this report:

- HTTP (Hypertext Transfer Protocol): It the underlying protocol used by the world wide web. It defines how messages are formatted and transmitted on the web.

- HTTPS (HTTP secure): It is a protocol for secure communication over a computer network.

- FTP (File Transfer Protocol): It is a protocol used for the transfer of files between two computers.

- SFTP: It is a secure file transfer protocol.

Management Action Plan

Control objective 1: Data transferring between primary and secondary care systems is complete and accurate.

1.1: Absence of service level agreement to resolve TRAKcare documents that are rejected by the EDT system	**Important**

Observation and risk

There is no formal service level agreement for the resolution of TRAKcare documents that have been rejected by the EDT system. At the time of our review, there was one rejected document that had not been cleared for more than a week. There was no clear expectation of when this document rejection would be fixed.

Microtech is the software vendor for the EDT system. This vendor is expected to identify these document transfer rejections and resolve them. Microtech does not usually report document rejection fixes to the eHealth system admin team. However, Microtech would ask the eHealth system admin team to retransmit a rejected record should this be required. Additionally, the eHealth system admin team has access to EDT Hub where the resolution of these rejection issues could be monitored.

There is a risk that data transfers rejected by the EDT system are not resolved within a reasonable period of time. This could lead to delays in the communication of exam results to patients.

Recommendation

We recommend that a service level agreement for the resolution of EDT rejected documents is agreed between eHealth and Microtech.

Management Response

EDT HUB is a national product which is managed for NHS Scotland by National Services Scotland.

The Management Action

The above suggestions will be passed onto NSS to liaise with Microtech, and determine what changes are possible.

Responsibility:	Target date:
Head of eHealth Operations	May 2017

1.2: Absence of automated controls within the ECS system to validate the accuracy and completeness of patient records extracted from the Vision/EMIS systems	**Important**

Observation and risk

There are no automated controls within the ECS system to confirm that patient records have been extracted completely and accurately from the Vision/EMIS systems, which are used in primary care. The Board relies upon Clinicians to manually check the ECS system on an ad hoc basis and report any issues in relation to the incomplete or inaccurate transfer of patient records to the ATOS service desk team.

There is a risk that patient records could not be extracted completely or accurately by ECS from Vision/EMIS and these went undetected or unreported by the Clinicians, resulting in medical decisions being based on inaccurate information. It should be noted that we did not identify any actual instances of this risk occurring.

Recommendation

We recommend that automated alerts are implemented to notify the ECS system admin team and the ATOS service desk team of any data transfer errors between the Vision/EMIS and ECS systems in order to increase the efficiency in the resolution of any potential data transfer issues.

Should these automated alerts be not feasible to be implemented, National Services Scotland should designate a team to monitor and resolve data transfer errors between Vision / EMIS and ECS on a regular basis.

It should be noted that the ECS system admin team sits within National Services Scotland (NSS).

Management Response and Action

ECS is a nationally managed application. These suggestions will be passed onto NSS who manage this system on behalf of NHS Scotland, but NHS Lothian can do no more than pass on these suggestions.

Responsibility: Head of eHealth Operations	Target date: May 2017

Control objective 2: Duplicate data transfers are not processed by the target system.
We found no significant weaknesses in relation to this control objective.

Control objective 3: Rejected data transfers are monitored and fixed on a timely basis.
We found no significant weaknesses in relation to this control objective.

- **Control Objective 4:** Data is transferred between primary and secondary care systems via encrypted and/or secure channels.

4.1 There are no encrypted communications in a number of interfaces between primary and secondary care systems.	**Important**

Observation and Risk

Although all data transfers between primary care and secondary care systems are made within the Scottish Government's Wide Area Network (SWAN), we noted that the following communications were not encrypted:

a) Data transfers between the TRAKcare and EDT systems are made via the HTTP protocol instead of HTTPS.

b) Data transfers between the TRAKcare, iLab and SCI store systems use FTP instead of SFTP. As a compensating control, we understand that the TRAKcare, iLab and SCI store systems sit in the same server rooms and network. Although this is deemed to be satisfactory for now, NHS Lothian should consider the implementation of encrypted communication links should any these systems be relocated in the future.

There is a risk that unauthorised access to patient data could be gained should a malicious intruder intercept the data transfers between primary and secondary care systems.

Recommendation

We recommend that NHS Lothian considers the implementation of HTTPS for the data transfers between the TRAKcare and EDT systems.

Management Response and Action

The revised configuration for communications between EDT Hub and TRAK will be completed by December 2017 to use SSL certificates, and so be secure.

TRAK Care, iLab and SCI Store sit in the same server rooms, on the same network. It is an unnecessary overhead encrypting systems sitting in the same room.

Responsibility:	Target date:
Head of eHealth Operations	December 2017 for EDT TRAK encryption. No action intended/required for other items.

- **Control Objective 5:** Logical access to interface functionality between primary care and secondary care systems is restricted to appropriate personnel.

5.1 A generic and privileged user account is shared by several teams to monitor the interface between SCI Gateway and TRAKcare	**Important**

Observation and Risk

A generic and privileged user account is shared by the clinical applications and technical services teams as well as Intersystems (software vendor) in the Ensemble Intersystems production system to monitor the interface between the SCI Gateway and TRAKcare systems. In addition, the password for this generic and privileged user account is not forced to expire. Although such access is required for these parties, they share a generic user account to perform this monitoring.

This generic account has access to all functionality within the Ensemble Intersystems production system. This includes the possibility of starting, stopping or changing the configuration of the interface. No financial information is passed via that interface.

We understand that there is an IT project within eHealth that would require users to authenticate to Ensemble via personal user accounts. This project is planned to start later this year.

There is a risk that the Board could find it difficult to hold members of staff accountable for any unauthorised actions performed in the Ensemble Intersystems production system.

Recommendation

We recommend that users of Ensemble Intersystems production system are authenticated via their personal user accounts. Additionally, the password of the generic and privileged user account should be forced to expire.

The activity of these privileged user accounts should be logged. The Board should implement a process to independently monitor the activity of these privileged user accounts on a regular basis.

Management Response and Action

It will be possible to implement these changes once the hardware used for Ensemble has been upgraded. This work is planned for completion by February 2018.

Responsibility:	Target date:
Head of eHealth Operations	February 2018

Control objective 6: Adequate electronic authorisation is provided for data transfers should it be required.
We found no significant weaknesses in relation to this control objective.

Appendix 1 - Definition of Ratings

Management Action Ratings

Action Ratings	Definition
Critical	The issue has a material effect upon the wider organisation – 60 points
Significant	The issue is material for the subject under review – 20 points
Important	The issue is relevant for the subject under review – 10 points
Minor	This issue is a housekeeping point for the subject under review – 5 points

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention (60 points and above)
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points)
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less)