Internal Audit

Datix System

June 2014

Report Rating	AMBER

Contents

Executive Summary

Report Rating	AMBER

Overall, a reasonable framework has been developed for managing the Datix system.

The Clinical Governance & Risk Management Support Team (CG&RMST) has developed procedures for administering Datix day-to-day, including granting access rights to users, resetting passwords, logging faults, running reports, answering queries and providing training. Meanwhile, eHealth provides technical cover for aspects such as supporting the server, software upgrades, back-ups and IT disaster recovery. As one of the largest corporate users of Datix, CG&RMST reports that good working relationships are maintained with Datix Ltd.

Nevertheless, certain aspects of how Datix is managed could be strengthened through some extra formality. For example, the process for granting access rights to Datix is not documented, and User Request Forms are not always held to confirm that users have been granted appropriate rights (issue 1). Also, user acceptance testing for system upgrades and changes has been conducted without set test scripts and without formal sign-offs from CG&RMST before changes go ahead (issue 2).

Although later found to be in order, CG&RMST could not evidence at the start of the audit that NHS Lothian held sufficient software licences for Datix or that the terms of the Service Level Agreement with Datix Ltd were adequate for NHS Lothian's needs (issue 3). Meanwhile, eHealth advises that ample capacity is available on the Datix server, although a strategy for archiving records from Datix is going to be required soon (issue 4).

CG&RMST comments that Datix is a low-risk system, with many of the issues raised in the report falling within accepted risk appetite. However, actions are to be taken to address specific points.

Background, Objective & Scope

Background

Datix is the risk management system used for reporting and monitoring risks, adverse events and near misses. Also, Datix is used to maintain risk registers and manage complaints and litigation cases.

The Datix system is provided under licence from Datix Ltd at a cost of circa [redacted] per year. The licence fee covers access to software upgrades and support on weekdays. The system is held on a dedicated server managed by eHealth, with eHealth overseeing software upgrades, back-ups and IT disaster recovery arrangements.

CG&RMST oversees the day-to-day operation of Datix. In particular, the team grants user-rights to the system, manages the hierarchy of NHS Lothian staff, delivers training and provides a Help Desk facility.

Objective

The objective of the audit was to evaluate the adequacy and effectiveness of internal controls for managing Datix.

The audit focused on specific control objectives.

- The Datix system is held on a secure server.
- User access rights are set appropriately.
- Performance and capacity are regularly monitored to address any limitations.
- System upgrades and changes are implemented in a controlled environment.
- System software and data are regularly backed up.
- Disaster recovery plans are in place.

Scope

The scope of the audit included:

- logical security and system administration;
- IT and user support;
- performance and capacity planning;
- licence agreements;
- data and software back-ups;
- system development and change management;
- user training and documentation; and
- business continuity and disaster recovery planning.

The scope excluded:

- system functionality and data integrity – separate audit.

Audit Issues & Recommendations

Issue 1 Significant	Access rights granted to Datix cannot be confirmed as being fully correct, and passwords do not conform with the Security Policy

All staff with access rights to NHS Lothian's network automatically gain access to log adverse events on Datix. Additional access rights to modules within Datix are granted by CG&RMST.

While the process is not documented and signatures are not checked, CG&RMST expects to receive User Request Forms authorised by line managers and submitted by post or, more usually, e-mail. Generally, access rights are granted based on staff members' roles and locations (eg specific wards or departments for Charge Nurses, Clinical Nurse Managers or Service Managers). When requests appear to be out of line with staff members' remits, CG&RMST would discuss the requests and seek clarification, although the rationale for decisions is not documented.

Although Datix has been in use since 2005, User Request Forms are only held for the past 18 months. Before this, access requests were made by e-mail which was considered sufficient at the time. Currently, paper copies of User Request Forms may be held at Pentland House or St John's Hospital or electronic versions may be held on the team's shared-drive.

During the audit, CG&RMST produced for Internal Audit a report listing new and amended user rights granted between January 2013 and April 2014. However, CG&RMST advised that the report was incomplete, as "effective from" dates are not always entered when access rights are granted. From the 123 names on the report, User Request Forms could not be found for 28 users (23%), although e-mails were found to support granting access to 19 staff. From reviewing 87 forms, the requests appeared to have been authorised correctly, with appropriate access rights granted based on staff members' roles and locations.

When staff leave NHS Lothian, network access is removed by Directory Services within eHealth. For staff with access to additional modules in Datix, line managers are expected to advise CG&RMST separately to revoke permissions. Although not documented or specifically scheduled, CG&RMST advises that each year the team checks for staff who have not logged on to Datix over the past 12 months. Recently, the team has introduced a procedure to remove access rights when undeliverable messages are received in response to all-user e-mails (eg notifying staff about opening hours for the Help Desk on public holidays).

The eHealth Security Policy requires that passwords to systems be a minimum of 6 characters long, with a mix of alphabetic and numeric characters. Also, the policy requires that systems force users to change their passwords after 42 days. While Datix can be configured to comply, currently passwords for Datix only need to be 4 characters long and changed every 90 days.

Without comprehensive procedures and records, access rights may be granted inappropriately. Also, passwords are more open to be compromised if the Security Policy is not followed.

Recommendation

Standard Operating Procedures should be developed to cover all aspects of granting and removing access rights to modules in Datix.

Datix should be configured to comply with the requirements for passwords as set out in the Security Policy.

Management Response

CG&RMST has an extensive range of Standard Operating Procedures to support staff who contribute to our Datix Help Desk. There is a Standard Operating Procedure to address the setting up or removal of users and on amending user permissions. These do, however, only cover the technical aspects of the tasks and do not cover aspects of checking the validity of the form submitted.

Management Action

Standard Operating Procedures have been amended to include the process which our staff follow. However, we are unaware of a comprehensive system which provides real-time information to validate requests. CG&RMST believe that the existing process which relies on the signature of the relevant line manager is sufficient and is in line with common practice within the organisation.

Datix has now been configured to comply with the requirements for passwords as set out in the Security Policy.

Responsibility:	Target date:
[redacted] Quality & Safety Assurance Manager	Complete

Issue 2 Important	User testing is conducted informally without formal sign-offs to confirm that system changes can go ahead

Datix is covered by eHealth's standard control framework for scheduling and monitoring system upgrades. Meanwhile, CG&RMST advises that good relationships and communication with eHealth supports current processes working well.

When upgrades are due for Datix, the new software is tested by NHS Lothian using a testing website. User testing is carried out by the main teams that use Datix, ie CG&RMST, Customer Relations & Feedback and Litigation. In the main, testing involves the teams running their usual processes, reports and queries within the test environment to confirm that no adverse changes have taken place. However, the testing is conducted informally, with no structured test scripts or sign-offs.

Changes to Datix are managed through eHealth's Assyst system, with eHealth only proceeding with updates following confirmation by telephone or e-mail from CG&RMST. However, formal sign-offs are not obtained from CG&RMST to confirm that changes can go ahead.

Without complete documents, the effectiveness of user-testing and sign-off of changes cannot be evidenced.

Recommendation

Standard Operating Procedures should be developed setting out the level of testing expected for system changes to each module of Datix. The procedures should make clear what sign-offs are required at each stage before changes are implemented.

Management Response

We consider this to be low risk – this is an internationally used off-the-shelf software package with any update or patch receiving extensive testing prior to release by the manufacturer.

Testing is based on the routine tasks carried out by users: filling in forms and running standardised reports. We feel that the measures that we already have in place are more proportional for routine software updates to an off-the-shelf software package. Even in the highly unlikely event of a failure, recovery plans are in place and the impact would be negligible.

Management Action

Not applicable.

Responsibility: N/A	Target date: N/A

Issue 3 Important	CG&RMST could not evidence that NHS Lothian held sufficient software licences or the adequacy of the Service Level Agreement with Datix Ltd

Datix is an off-the-shelf system which NHS Lothian has been using since 2005. In February 2014, NHS Lothian paid Datix Ltd an annual charge of [redacted] (including VAT) for continued use of Datix, including customer support.

While a generic Software Licence is published on Datix Ltd's website, CG&RMST did not hold any documents relating to NHS Lothian's original purchase of Datix, including the number of users or sites permitted. CG&RMST believes that original documents were destroyed by a former manager when responsibility for Datix transferred to the team in 2012. Following discussions with Datix Ltd in November 2013, CG&RMST has obtained confirmation that current licence arrangements are sufficient for NHS Lothian.

Also, CG&RMST did not hold a copy of the Service Level Agreement with Datix Ltd regarding levels of customer support. However, a copy of the Service Level Agreement was obtained during the audit.

CG&RMST logs system faults on to the website of Datix Ltd, with e-mails received from Datix Ltd quoting estimated times for resolution. Until the audit, the team did not keep any internal logs of faults reported to Datix Ltd, with no monitoring against the Service Level Agreement. A spreadsheet to monitor faults has now been set up.

Although CG&RMST reported no problems in any of these areas, the team was unable to confirm that important aspects were in order.

Recommendation

The issues were addressed during the audit.

Management Response

We employ one Datix Systems Administrator in NHS Lothian. We have a positive working relationship with Datix Ltd. Should any service quality or support issues arise, even on a case-by-case basis, this would quickly be escalated to the Datix Business Manager.

Again, our view is that this is low risk – we have not experienced any problems which have not been quickly resolved.

Management Action

Not applicable.

Responsibility: N/A	Target date: N/A

Issue 4 Important	Information may be held on Datix for longer than is appropriate

eHealth advises that ample capacity exists on the Datix server, with potential to extend capacity or move Datix on to a larger server, if necessary.

During the audit, eHealth advised that a performance or capacity issue may arise due to the increasing number of documents attached to incidents recorded in Datix. In particular, attachments are stored on a certain drive on the Datix server but not in any particular order. When documents need to be retrieved, Datix requires to search through each document until the required document is found. As more and more documents are stored, eHealth comments that locating documents is likely to take longer and lead to slower system performance.

NHS Lothian began using Datix in 2005, with no records yet having been archived from the system. NHS Lothian's Records Management Policy requires that specific categories of incidents, complaints and litigation cases be held for 10 years before being destroyed. As the 10-year anniversary of using Datix approaches, a strategy for archiving documents from Datix is going to be required, especially as some records within Datix may hold personal data.

Without planning ahead, future problems may be encountered with system performance and compliance.

Recommendation

An archiving strategy should be developed for identifying and removing information that is no longer required. Thereafter, information should be archived regularly and system performance closely monitored.

Management Response

It should be noted that the issue identified above relating to the way documents are stored is a technical, background issue within the software which does not impact on end-user experience or ability to locate documents. The way the software manages this function could only be changed by the software developer / manufacturer.

We have previously asked Datix Ltd to review if archiving is necessary to improve or maintain performance, however, they have responded that this is not necessary.

Agreed that documents should be removed in terms of compliance with NHS Lothian's Records Management Policy. A review and plan is required, although exceptions around information relating to claims will need to be considered. For example, records relating to adverse events since 2008 when a child has been affected must be held for 6 years after a case has been closed. If a legal judgement is made that a case must remain open, records must be retained indefinitely. Information on adverse events and complaints requires to be held for a longer period of time in respect of the potential for future litigation. For example, an adverse event which occurs relating to a birth has the potential to feature in a future claim and this could happen any time up until their 25th birthday.

Management Action

A review and plan will be developed to comply with the Records Management Policy, although some exceptions may have to be applied.

Responsibility: [redacted] Quality & Safety Assurance Manager	Target date: 31 December 2014

Definition of Ratings

Report Ratings

- Red – 40 points or over.
- Amber – 20 to 35 points.
- Green – 15 points or less.

Issue Ratings

- Critical – 40 points – the issue has a material effect upon the wider organisation.
- Significant – 10 points – the issue is material for the subject under review.
- Important – 5 points – the issue is relevant for the subject under review.

Audit Team

[redacted], Principal Auditor
[redacted], Chief Internal Auditor

Distribution List

Tim Davison, Chief Executive
Susan Goldsmith, Director of Finance
David Farquharson, Medical Director
Alex McMahon, Director of Strategic Planning, Performance Reporting & Information
Alan Boyter, Director of Human Resources & Organisational Development
Alex Joyce, Employee Director
Martin Egan, Director of eHealth
Stuart Wilson, Director of Communications & Public Affairs
[redacted], Clinical Governance Manager
[redacted], Quality & Safety Assurance Manager
[redacted], Server Analyst
[redacted], System Administration Manager
Audit Scotland, External Audit

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.