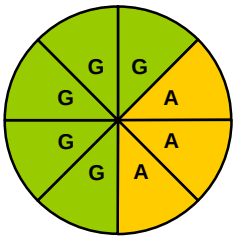
Internal Audit

TrakCare Application

October 2015

Report Assessment



Contents

Introduction

TrakCare is the electronic patient management system used across NHS Lothian's Acute and Community divisions to record and store information for patient consultations, investigations and treatments. TrakCare links to other systems such as iLabs, PACS (for the ordering of patient tests and electronic transmission of results) and the Interagency Information Exchange that shares information with the four Local Authorities.

Information recorded on TrakCare is widely used by all levels of management for performance monitoring and decision making purposes, for example in the management of waiting lists and bed management.

Availability of access to the TrakCare system is critical to the day-to-day running of the organisation as is ensuring that the confidentiality of the patient information recorded is maintained and accessible only to authorised personnel. In addition, the eHealth Paper Lite Programme has an objective to reduce the amount of patient information held in paper case notes by moving towards a scanned electronic version which will be held on TrakCare.

Scope

We reviewed the physical and logical security controls in place that ensure the confidentiality, integrity and availability of the system data. The review also considered controls in place for managing system developments.

The control objectives for the audit are set out in the Management Action Plan, along with our assessment of the controls in place to meet each objective.

Acknowledgements

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

Executive Summary

Conclusion

The control framework surrounding TrakCare is generally robust and effective. However, we have identified some areas where existing controls can be enhanced and where further examples of best practice can be incorporated.

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	There are adequate system administration and user procedures.	Green	-	-	-	1
2	There are robust logical access controls.	Amber	-	-	2	1
3	There is effective user account management which ensures only authorised users have access, including restrictions on users with access to amend system parameters.	Amber	-	2	-	-
4	User access levels are appropriate and ensure adequate segregation of duties in relation to the administration and operation of the system.	Amber	-	1	1	-
5	All data interfaces ensure complete and accurate transfer of data.	Green	-	-	1	-
6	Adequate backup, recovery and continuity procedures are in place.	Green	-	-	1	-
7	There are audit facilities within the system to allow effective and regular monitoring of the application.	Green	-	-	1	-
8	Change management procedures for system developments are in place and followed by staff.	Green	-	-	-	-

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:

eHealth has a dedicated team which is responsible for supporting the TrakCare application. This includes areas such as providing access to new users, training and follow on support where required. eHealth also has a large technical team who can quickly deal with errors and enquiries to ensure that TrakCare remains available and performs optimally.

To support both system maintenance and system users, eHealth has developed a comprehensive suite of documentation. This includes standard operating procedures (SOPs) for key tasks performed within eHealth as well as training materials and user guidance. These are available on the intranet and training staff are available to support users when required.

The application and supporting infrastructure for TrakCare has been designed to be highly resilient. This will reduce the risk of the system being unavailable and/or patient data being lost. We were pleased to note that a disaster recovery test has been scheduled for the TrakCare application which seeks to confirm that resilience works as planned, although we have raised a recommendation to ensure that this is subject to regular testing.

Controls exist to ensure that there is appropriate segregation of duties for the release of new TrakCare developments. The controls in place ensure that only authorised changes are promoted to the live environment.

In addition, the TrakCare application and systems integrated with TrakCare have an audit function which ensures that every transaction that is entered into these systems is attributable to a named individual.

We identified three significant areas for improvement during the review. These are listed below:

- Access to TrakCare requires users to have access to an active NHS Lothian network account. The Human Resources department should provide monthly reports to eHealth detailing staff leaving the organisation so that network access can be removed. We found that the reports had not been issued, or had been issued up to two months later than required, resulting in delays in removing network access.

- Managers must complete and sign a User ID request form for each member of staff who requires access to the TrakCare application. The authorised request forms should be retained by eHealth as evidence of a manager's authorisation for a staff member to be given access to TrakCare. We found that 13 forms were not available for users included in our test sample of 20 (65%).

- The number of users who have been assigned the 'System Administrator' role is excessive. At the time of our audit, over 150 users had been assigned this role which provides privileged access to TrakCare including the ability to create, amend and delete users as well as to allow limited configuration changes and management of waiting times. eHealth has advised that they plan to review the number of users with such access.

Further details of each of these points, as well as eight less significant issues, are set out in the Management Action Plan.

Management Action Plan

Control objective 1: There are adequate system administration and user procedures	
1.1: Not all eHealth documentation has review dates.	**Minor**
Observation and Risk eHealth has developed a comprehensive suite of documentation for TrakCare. This includes TrakCare User Account Management SOP, TrakCare Business Continuity Plan and a range of user guides and training materials. These are available to eHealth staff on the eHealth shared drive and to end users via the intranet. We noted that the majority of TrakCare documentation contain details of the reviewer as well as the date of the next review. However, some do not contain this information, namely the TrakCare Training documentation and the Backup & Recovery Strategy for the TrakCare Patient Management System. If documentation is not reviewed periodically there is a risk that information is not up-to-date and guidance does not reflect current practices.	
Recommendation eHealth should ensure that all formal documentation includes all key document management information, including date of creation, author, reviewer, approver, and the next review date.	
Management Response and Action Documentation currently not containing this information will be amended accordingly.	
Responsibility: [redacted] Systems Administration Manager	Target date: 29/01/2016

Control objective 2: There are robust logical access controls	
2.1 TrakCare allows multiple simultaneous logons.	**Important**

Observation and Risk

We identified that the current configuration of TrakCare system parameters allows for users to have multiple active sessions. This means that users can access TrakCare from multiple workstations at the same time. Although system parameters allow concurrent logins to be disabled this option has not been activated.

By allowing users to have multiple logins to TrakCare at the same time there is a risk that they leave workstations where they have active sessions unattended. This could result in their user account being misused and provide access to sensitive clinical data to unauthorised users / members of the public.

Recommendation

eHealth should consider the activation of the system parameter which restricts users to a single active login to TrakCare. Where clinical need means that more than this is required, eHealth management should remind users to ensure that their workstations are locked to prevent any unauthorised use.

Management Response

This setting was recently enabled, however it had an adverse effect on functionality that used the TRAK API. This has been disabled again and eHealth are in discussion with InterSystems about how to exclude these system accounts from this restriction.

Management Action

Follow up with InterSystems to determine if there is a way to exclude certain accounts from this restriction. If not, we will raise a change request for a future version of TrakCare to allow this.

Responsibility:	Target date:
[redacted] Systems Administration Manager	31/12/2015

2.2 TrakCare does not enforce the use of complex passwords.	**Important**
Observation and Risk NHS Lothian Security Policy – Password Management requires that, where an application permits, passwords should have a minimum of six characters which include at least one non-alphabetic character. TrakCare has the facility to enforce password complexity however, this has not been activated. Instead users are encouraged to select a password which includes non-alphabetic characters. There is a risk that users will not implement guidance and select weak passwords. The use of weak passwords increases the risk of unauthorised personnel gaining access to the TrakCare application.	
Recommendation eHealth should activate the parameter within TrakCare to force the use of complex passwords which include at least one non-alphabetic character.	
Management Response This function will require to be tested in order to ensure it is fit for purpose. If it passes the testing then extensive communication to users will be required before enabling this. Management Action Undertake testing programme and progress to Live when appropriate.	
Responsibility: [redacted] Systems Administration Manager	Target date: 29/01/2016

2.3: Forced password change periods are not in line with NHS Lothian procedures.	**Minor**
Observation and Risk The eHealth Standard Operating Procedure – Systems Account Allocation, Password Reset and Deactivation Management Procedure requires that, where a system permits, user passwords should be changed every 28 days. The aim of the procedure is to establish a consistent approach to systems password management across NHS Lothian. However, we identified that in practice passwords for TrakCare (and network access) have been set to force a password change every 42 days which is not in compliance with the Standard Operating Procedure. If passwords are not changed on a regular basis, there is an increased risk that they will become known to unauthorised users resulting in the potential for misuse/abuse of user accounts. This could result in data integrity being undermined.	
Recommendation eHealth should either change the Standard Operating Procedure – Systems Account Allocation, Password Reset and Deactivation Management Procedure to state that passwords should be force-changed every 42 days, or TrakCare should be adjusted to require users to change their passwords every 28 days.	
Management Response and Action The SOP will be amended to reflect that of Active Directory which is 42 days.	
Responsibility: [redacted] Systems Administration Manager	Target date: 30/11/2015

Control objective 3: There is effective user account management which ensures only authorised users have access, including restrictions on users with access to amend system parameters	
3.1: Authorised user ID requests are not held for all users.	**Significant**
Observation and Risk In order to access TrakCare, approval must first be provided by the staff member's line manager. The line manager completes and signs a User ID request which is used by eHealth Systems Administration team to determine the correct level of access for the user, with the completed requests then being held centrally by eHealth Directory Services. In addition, the NHS Scotland IT Security Policy recommends that user access rights be reviewed every six months. However, for a sample of 20 active users, we could only locate seven forms. eHealth advised that five users were possibly given access as part of the Mental Health Migration project and forms were not yet filed. However, for the remaining eight users, there was no obvious reason for the forms not to be present. Without evidence of line manager authorisation for TrakCare access there is reduced confidence that TrakCare is being accessed appropriately, and that the NHS Scotland IT Security Policy is being complied with.	
Recommendation eHealth Systems Administration team should provide the eHealth Directory Services team with a list of all new system access accounts created in each month. eHealth Directory Services should reconcile the list to authorised User ID request forms held. eHealth Directory Services should follow up with eHealth Directory Services any cases where access has been given and no authorised request held.	
Management Response & Action eHealth are currently undertaking a review of user account provision for TrakCare and other applications, which will encompass this. Historic User access forms are to be scanned and indexed to allow for better and easier retrieval. Alongside the review a new SOP will be developed for User account provision. A number of the "missing" forms from the sample were created by trainers and therefore likely to be in the batch of forms not yet scanned by Directory Services.	
Responsibility: [redacted] Systems Administration Manager	Target date: 04/03/2016

3.2 Network accounts for leavers are not disabled in a timely manner.	Significant

Observation and Risk

Access to TrakCare requires users to have access to an active NHS Lothian network account. The Systems Account Allocation, Password Reset and Deactivation Management Procedure requires that HR issues monthly leavers reports to eHealth to enable them to disable / remove network accounts.

Our review of HR leaver reports for the months December 2014 – July 2015 showed that only two of the eight reports had been provided to eHealth within the correct timeframe. One was one month overdue and one was two months overdue. For two months no reports had been issued. In addition, eHealth advised that staff shortages within Directory Services have meant that the scheduled audits of network accounts that have been inactive for at least 90 days have not being carried out in full for around a year.

While it is the responsibility of line managers to advise eHealth when a staff member's TrakCare access should be removed, this does not always happen. To reduce the risk of inappropriate access to TrakCare, on a daily basis the eHealth System Administration team disables TrakCare user accounts which have been inactive for the past 90 days.

However, we noted that the removal of access to an individual's network account does not automatically disable their access to TrakCare. There is no direct link between a user's network and TrakCare account. As a result, even when a network user account is disabled or deleted, the user account could still be used to gain access to TrakCare – whether this be through the owner of the account taking advantage of an open network session or an existing user gaining unauthorised access to the leaver's account.

While the control within the eHealth System Administration team to disable TrakCare accounts that have been inactive for 90 days was found to be operating effectively, there remains a 90 day period where user accounts of leavers could be compromised and unauthorised access gained to TrakCare. This could result in patient-sensitive information being viewed, amended or deleted inappropriately.

Recommendation

Line managers should be reminded of their responsibility to notify HR as well as all relevant system administrators of leavers.

eHealth should also liaise with HR Systems team to investigate the potential for leavers reports to be provided on a daily or weekly basis. Copies of the reports should be issued to the Directory Services and System Administration teams to allow user access to the network and TrakCare respectively to be disabled. This compensating control will further reduce the risk of user accounts being misused after a user has left the Board.

In addition, as a further compensating control eHealth should schedule regular audits to identify and then disable network user accounts which have been inactive for 90 days.

The Systems Account Allocation, Password Reset and Deactivation Management

Procedure should be updated to reflect any resultant changes in practice. It should also include a process to follow up the non-receipt of leavers reports from HR.	
Management Response This process relies on accurate and timely information from HR. Currently only network accounts are disabled as we also do not have any reference to tell us which network account belongs to which TRAK user account. As a consequence all TRAK accounts are automatically disabled after 90 days of inactivity. Management Action eHealth will review the current process with a view to implementing the above recommendations.	
Responsibility: [redacted] Systems Administration Manager	Target date: 04/03/2016

Control objective 4: User access levels are appropriate and ensure adequate segregation of duties in relation to the administration and operation of the system	
4.1: System administration access rights are not reviewed.	**Significant**

Observation and Risk

System access rights vary according to the user's roles and responsibilities. For example, the majority of users will have access to view and update patient information. Access to change system functionality or system parameters, or perform tasks such as management of waiting times information will typically be more restricted. Such access is granted through the 'System Administrator' role. We noted that there are approximately 150 users who have been assigned this role.

Although controls are in place and working effectively to prevent unauthorised changes being made to TrakCare, eHealth has recognised that the number of users who have been assigned the 'System Administrator' role is excessive and is planning to review this.

Best practice recommends that user access to applications is subject to regular review (no less frequently than every 6 months). This is to confirm that user access remains valid to their role and responsibilities. We noted that no such review has been undertaken. eHealth explained that, while the location of individual users can be identified from the application, there is no data to identify the user's line manager. As a result, it is inherently difficult to conduct such reviews.

Without reviewing user access permissions there is a risk that users have access which exceeds their role and responsibilities. This could result in patient information being accessed, amended or deleted inappropriately. There is also a risk that, by not effectively controlling access to roles with privileged access permissions, this could result in unauthorised changes being made to system parameters and users accounts being created, amended or deleted.

Recommendation

eHealth should carry out the planned review and ensure that only those users with a business need are assigned the 'System Administrator' role. Consideration should be given to the creation of additional role profiles based on the system's administrator role but with permissions which are commensurate with their roles and responsibilities for users who do not require all access privileges granted through the 'System Administrator' role.

eHealth should also investigate a means through which user access levels can be subject to regular review. For example, consideration should be given to liaising with Payroll and HR to determine an efficient method of locating TrakCare users' line managers to obtain confirmation that their staff require access to TrakCare and that access levels are appropriate. This could be through existing common information or the introduction of a common location code.

Management Response A System Admin access review has started and will address this concern. Once completed our recommendation is that a review of staff with System Admin access is carried out annually as we currently do for InterSystems staff access. We do not think it's practical, nor possible without much better HR data and resource, to review permission levels for all TRAK System Users at a fine level of granularity. Management Action Complete the System Admin access review.	
Responsibility: [redacted] Systems Administration Manager	Target date: 31/03/2016

4.2: There is no Access Matrix of permissions within each security group.	**Important**

Observation and Risk

The level of access granted to individual users is determined by eHealth and is based upon their role in the organisation. eHealth has created approximately 80 individual role 'profiles' which are specific to particular roles / tasks. Each user will be assigned at least one role profile and this determines their level of access to TrakCare. This approach is good practice as it reduces the administrative burden associated with maintaining the system and more closely controls user access.

Currently, assignment of role profiles to user accounts is reliant on local knowledge within eHealth. There is no documentation which explains the process to be followed for determining access rights. There is also no document or access matrix which acts as a decision-making tool in defining user access permissions.

Furthermore, we noted that there has not been any formal review of the current role profiles to confirm that they remain relevant and ensure that access is based on the need-to-have / need-to-know principle.

There is a risk that local knowledge could be lost if staff leave the Board or move to different roles. The absence of periodic review of the job profiles may result in users having access permissions which exceed the requirements of their role. This could result in access being provided to patient-sensitive data where there is no business requirement for this.

Recommendation

eHealth should document the process for determining access rights. The document should include a matrix which explains the permissions granted to users within each security group. The documented process will facilitate a consistent approach to determining appropriate access rights and reduce the current reliance upon local knowledge.

A review of existing role profiles should be undertaken to ensure that they remain relevant. Where role profiles are no longer required they should be disabled or deleted to prevent them from being assigned to current or new users. In addition, where the review requires that changes are required to roles, these should be managed through the Change Configuration and Release change management process (CCR) to ensure that the risk and impact of these are fully tested and understood.

Management Response

System access is currently reviewed as new features are rolled out and significant changes made to existing functionality.

Management Action	
eHealth will produce a SOP for determining access rights and a document detailing the roles to be assigned to each security group. An annual review of role profiles will be implemented and documented.	
Responsibility: [redacted] Systems Administration Manager	Target date: 29/01/2016

Control Objective 5: All data interfaces ensure complete and accurate transfer of data	
5.1: Error logs are not maintained and monitored.	**Important**
Observation and Risk The day-to-day operation of TrakCare involves a significant number of tasks including interfaces with other clinical systems and maintenance tasks. There are occasions where tasks do not complete correctly. When this is the case error messages are generated and eHealth is notified by email/SMS. eHealth will then take action to resolve the error. However, although the system records errors and produces error messages, eHealth does not independently record or monitor the volume and type of error messages to identify trends. If error messages are not documented and analysed there is a risk that trends are not identified and the opportunity for the identification of potential problems is missed.	
Recommendation TrakCare error messages should be recorded as service desk tickets and monitored by the eHealth team. Trends should then be identified from this information in order to identify recurring issues which may be indicative of a problem.	
Management Response and Action The interfaces are currently monitored and alerts are configured. The errors mentioned here vary from patient specific errors (the vast majority of iLab interface errors are down to different demographics in systems) to system error (cannot connect to another system). eHealth will review existing interface monitoring processes to ensure they are robust. Logging each error on the service desk would take significant resource which Sys Admin do not currently have and for little perceived benefit.	
Responsibility: [redacted] Systems Administration Manager	Target date: 29/01/2016

Control Objective 6: Adequate backup, recovery and continuity procedures are in place	
6.1: Business Continuity Plans have not been tested.	**Important**
Observation and Risk The eHealth Business Continuity Plan contains the detailed recovery steps that need to be taken to restore the individual IT systems that eHealth support. The TrakCare disaster recovery plan is included in the Business Continuity Plan. Service areas using TrakCare are responsible for the development of their own business continuity plans. While the TrakCare Disaster Recovery Plan is regularly reviewed it had not been tested at the time of this audit. However, eHealth has developed a plan to perform failover testing of aspects of the TrakCare system to provide assurance with regard to system resilience. If regular testing of the Disaster Recovery Plan is not undertaken, there is a risk that the plans will not support the effective and efficient response to a disaster. This could therefore result in delays to restoring business critical systems.	
Recommendation eHealth should ensure that the disaster recovery testing of TrakCare is performed as planned. The results of the test should be documented with all actions (including updates to the detail within the plan) recorded and tracked to ensure that they are resolved.	
Management Response and Action The planned testing due to take place in October was delayed due to operational reasons and has being re-scheduled for November 2015. The TRAK business continuity plan will document the process and frequency for testing of these plans, it is anticipated that this will be carried out every 6 months.	
Responsibility: [redacted] Systems Administration Manager	Target date: 31/12/2015

Control Objective 7: There are appropriate audit facilities within the system to allow effective and regular monitoring of the application	
7.1: Actions to address findings from Intersystem reviews and system health checks have not been recorded.	**Important**
Observation and Risk In August 2015 Intersystems, the TrakCare System Developers performed reviews and health checks of the TrakCare application and infrastructure in order to assess the current system's capabilities, as well as the resource requirements for the proposed system upgrade from the current T2012 version to T2016. Intersystems produced a report for each review carried out. The reports used a traffic light system to grade findings and included recommendations. While eHealth has confirmed that the reports have been reviewed and discussions are underway to address the findings, an action plan has not been documented. Without documentation to evidence decisions and actions taken in response to the Intersystems report. there is a risk that recommended improvements may not be made. This could result in TrakCare not being fully secured or operating at optimal configuration.	
Recommendation eHealth should develop a formal action plan which documents the response to each recommendation contained within the Intersystems reports. Each action should be allocated a responsible officer and an implementation date. Where action is not being taken, the reason for this should be documented. Progress against the action plan should be subject to formal monitoring within eHealth (or a TrakCare governance group if such a thing exists).	
Management Response and Action The InterSystems report has been reviewed and a report is being produced to document our response and anticipated actions.	
Responsibility: [redacted] Systems Administration Manager	Target date: 31/12/2015

Control Objective 8: Change management procedures for system developments are in place and followed by staff.
We identified no significant issues in relation to this control objective. NHS Lothian has change management procedures in place. These procedures are subject to regular review to ensure they remain up-to-date. All changes are managed through the CCR Change Management System. This includes setting out each key stage of the change, using standard documentation. Progress against changes is monitored regularly via the weekly Trak Change meetings. All changes are reviewed prior to being introduced in the live environment; changes cannot go live until they have been signed-off. Larger change projects are managed through the Trak Project Board, which includes representation from the provider, Intersystems.

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)