Internal Audit

Information Governance

February 2018

Internal Audit Assurance assessment:

Objective One	Objective Two	Objective Three	Objective Four	Objective Five	Objective Six
Significant Assurance	Moderate Assurance	Significant Assurance	Moderate Assurance	Significant Assurance	Significant Assurance

Timetable

Date closing meeting held: 19 January 2018

Date draft report issued: 5 February 2018

Date management comments received: 15 February 2018

Date Final report issued: 23 February 2018

Date presented to Audit and Risk Committee: 23 April 2018

Contents

Introduction 3
Executive Summary 4
Management Action Plan 8
Appendix 1 - Definition of Ratings 19

Introduction

Information represents one of the major assets held by any organisation. The efficient, effective delivery of services is dependent on the maintenance of up-to-date, complete, accurate and properly secured information.

Information Governance is a set of policies, procedures, processes and controls implemented to manage information in such a way that it supports an organisation's immediate and future regulatory, legal, risk environmental and operational requirements.

NSH Lothian is required to comply with a number of Information Governance Standards including Caldicott Guardian (CG) requirements, the Data Protection Act 1998 (DPA), and the Freedom of Information (Scotland) Act 2000 (FOI). Additionally the Data Protection Act is being replaced by the General Data Protection Regulations (GDPR), which comes in to effect from the 18 May 2018. NHS Lothian have established a Short Life Working Group (SLWG) to determine the actions that need to be taken in advance of the regulations coming in force, and internal audit are providing challenge and observations through membership of this group. Additionally a review of GDPR compliance is planned for 2018/19.

NHS Lothian is also required to demonstrate compliance with the requirements of the Public Records (Scotland) Act 2001 (PRA), and has done so through the creation of a Records Management Plan, which was submitted to the Keeper of the Records of Scotland at the end of April 2016. This has been reviewed by the Keeper and on 4 April 2017 a response was received by NHS Lothian from which identified some improvement opportunities.

On 27 May 2016, the Information Commissioner produced a report from a data protection audit of NHS Lothian carried out earlier in the year. A number of corrective actions were identified and incorporated into an action plan.

Scope

This review sought to ensure the controls in place to govern the use of information are in line with legislative and regulatory requirements, and are adequate and effective. Our review focused on controls around compliance with the Data Protection Act 1998, Freedom of Information (Scotland) Act 2002, Public Records (Scotland) Act 2011 and Caldicott Guardian guidance.

Acknowledgements

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

Executive Summary

Summary of Findings

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

No.	Control Objectives	Assurance Level	Number of findings			
			Critical	High	Medium	Low
1	An Information Governance Policy and Strategy is in place that sets out the controls for the management of information assets.	Significant Assurance	-	-	-	-
2	An Information Governance Framework is in place and includes controls that support, compliance with the DPA, FOI, CG and PRA.	Moderate Assurance	-	1	1	-
3	Management monitors compliance with the Information Governance Framework and reviews performance against it.	Significant Assurance	-	-	-	-
4	New and existing staff members receive training about Information Governance Policies and Procedures.	Moderate Assurance	-	-	1	-
5	Actions arising from the submission of the Records Management Plan and Information Commissioners Audit are being addressed.	Significant Assurance	-	-	-	-
6	The Healthcare Governance Committee receives regular reports about management actions to identify, investigate, report and address non-compliance with legal and regulatory responsibilities for Information Governance.	Significant Assurance	-	-	-	1

TOTAL			**-**	**1**	**2**	**1**

Conclusion

There is a framework in place designed to provide senior management and staff with instruction and guidance around information governance, while supporting legislative compliance. However, we identified areas for improvement relating to meeting attendance, information asset risk assessments completion of mandatory training and the governance structure.

Main Findings

A formal Information Governance Policy is in place which provides guidance to all staff on the implementation of effective information governance. The Policy also includes arrangements to promote compliance with the DPA, FOI and CG legislation, and how NHS Lothian will adhere to the requirements of the PRA. All relevant information governance policies and procedures are easily accessible to all staff via the Information Governance Intranet webpage.

The Scottish Government has recently withdrawn the requirement for NHS Boards to maintain an Information Assurance Strategy beyond the introduction of GDPR in May 2018. Instead, existing policies and procedures will be considered sufficient in ensuring that there is a robust control framework around information governance. Which the review and update of will ensure compliance with the GDPR requirements.

Roles and responsibilities for information governance activities are clear. There are designated Directors in place for all areas of information governance. There is also a dedicated Information Governance Team, which provides advice and guidance as required.

The Healthcare Governance Committee (HGC) has overall ownership for information governance monitoring and scrutiny, with the responsibility for monitoring performance against the information governance framework delegated to the Information Governance Assurance Board (IGAB), which is a sub-committee of the HGC and meets quarterly. To support the IGAB operationally there is also an Information Governance Working Group (IGWG) in place, which also meets quarterly, with minute for this group provided to the IGAB. IGAB meetings are chaired by NHS Lothian's Director of Public Health and Health Policy, with a number of senior management staff scheduled to attend the meetings (including the Employee Director, Information Governance & Security Manager, and Associate Director of Human Resources).

The Information Governance & Security Manager submits annually a summary report to the Audit & Risk Committee on the level of assurance provided by the IGAB. No significant issues had been reported and the Audit & Risk Committee agreed to accepted the level assurance to the Audit & Risk Committee in June 2017.

The IGWG is presented with several reports at each of its meetings, advising group members on a number of aspects of information governance. These include IT Security, inappropriate

access (through Fair Warning monitoring), and freedom of information and subject access requests. All requests received are closely monitored to prevent potential breaches of processing timescales.

NHS Lothian uses Datix to record and act on instances of non-compliance with information governance guidance. Non-compliance is also identified through complaints and issues raised through the Information Commissioner's Office (ICO).

From our sample testing the processing of Caldicott Guardian information access requests appears to be controlled, with all requests reviewed as part of this audit completed in full and approved by the Director of Public Health & Health Policy.

Freedom of Information Requests are generally being processed within relevant timescales and information released only following appropriate senior management review and approval.

The current timeline for responding to subject access requests is 40 calendar days. For the three months covering July to September 2017, 51 requests received for the RIE, WGH, SJH and LCTC (6% of the total of 835) had breached the 40 day timeline, with 47% of these attributable to issues from the medical notes scanning project and delays receiving approval from consultants. It is noted that for the three months covering April 2017– June 2017, 27% of all subject access requests processed through the Medical Legal department were completed after 30 days (data for July-September was unavailable), indicating that some work is necessary to meet with the requirements.

All staff are required to undergo formal training in information governance. All new staff must undergo a corporate induction process, which includes key elements of information governance requirements. Ongoing information governance training is provided through the online LearnPro module. In addition, the Information Governance Team provides regular Information Governance Roadshows across the organisation. LearnPro module content is being reviewed and updated to reflect the GDPR requirements.

The Keeper of the Records of Scotland has indicated there are no elements within NHS Lothian's Records Management Plan where there is a serious gap in provision.

The Information Commissioners Office undertook a follow-up audit in January 2017 and confirmed that the majority of actions from their original audit had been completed and evidenced. All outstanding issues have been addressed and the ICO is happy with the Board's progress.

We identified four issues during this review:

- Attendance at the IGAB and IGWG meetings is low, averaging 49% and 60% for the first three meetings of 2017.

- No controls are in place to confirm reassessment of information assets according to their risk rating.

- Completion of mandatory training in some areas is below Board target of 80%, for example the Edinburgh Partnership, General Medical Services has a 53% completion rate, from a head count of 157.

- The governance structure for Information Governance involves a sub-committee and a working group As a result the Healthcare Governance Committee may not have overall responsibility for Information Governance, increasing the risk that relevant matters are not included, reported, or receive sufficient attention.

Management Action Plan

Control objective1: An Information Governance Policy and Strategy is in place that sets out the controls for the management of information assets.
We identified no significant weaknesses in relation to this control objective. NHS Lothian has an Information Governance Policy in place. The Policy is published on the intranet and available to all staff with intranet access. The Policy was updated and approved by the Information Governance Assurance Board in July 2015 and will be reviewed and updated as required by the GDPR Short Life Working Group prior to the May 2018 GDPR deadline The Policy was reviewed and confirmed that it included relevant information, such as the purpose, scope and principles of NHS Lothian's information governance activities. It also set out how the Policy would be implemented and the governance structure in place to apply the principles of information governance throughout NHS Lothian. NHS Lothian also has an Information Assurance Strategy which has been developed to set out the high level framework within which the Board can monitor NHS Lothian performance and compliance in Information Governance, and provide an overview of responsibilities and sources of guidance for staff. NHS Lothian's Information Assurance Strategy follows the content and structure of the NHS Scotland Information Assurance Strategy, published under CEL 26 (2011) in November 2011 and implemented by NHS Boards. The Strategy was approved by the Director of Public Health and Health Policy in April 2013 and had been due for review. However, the Scottish Government has recently withdrawn the requirement for NHS Boards to maintain an Information Assurance Strategy beyond the introduction of GDPR in May 2018. Instead, existing policies and procedures will be considered sufficient in ensuring that there is a robust control framework around information governance. Which the review and update of will ensure compliance with the GDPR requirements.

Control objective2: An Information Governance Framework is in place and includes controls that support, compliance with the DPA, FOI, CG and PRA. **Associated risk of not achieving the control objective: Matters relating to effective information governance are not discussed and communicated effectively throughout the organisation.**	**High**

Observation and risk

The Information Governance Policy outlines the responsible directors and managers for DPA, FOI, PRA and CG legislation.

In addition, a dedicated Information Governance Team is in place, headed by the Information Governance & Security Manager. The Information Governance Team provides training, advice and guidance on complying with information governance legislation, policies and standards.

Overall governance on the management of information throughout NHS Lothian is provided by the Information Governance Assurance Board (IGAB) and Information Governance Working Group (IGWG). The IGWG is responsible for operational matters pertaining to information governance. The IGWG reports directly to the IGAB, which is responsible for more strategic aspects of information governance.

Both groups meet quarterly, with the IGWG feeding into the IGAB meetings. However, the meetings are reporting low rates of attendance, with IGWG recording an average of 60% attendance at its three meetings in January, April and July 2017. The IGAB recorded attendance at 49% over the same period.

Without reasonable representation at the IGAB and IGWG meetings, there is a risk that matters relating to effective information governance are not discussed and communicated effectively throughout the organisation.

Recommendation

Management should review the membership of the IGAB and IGWG and advise members of the requirement to attend meetings where possible.

Considering the introduction of GDPR regulations in May 2018, it is advised that the remit of these groups are also reviewed to ensure that the governance arrangements and reporting structure is appropriate.

Management Response

This recommendation is accepted, although it should be noted that the IGAB was reconstituted in January 2018 and will, on behalf of the Healthcare Governance Committee seek assurance that the Board has arrangements in place to effectively discharge its information management and governance responsibilities.

The GDPR short-life working group has also been convened to review the organisations

preparedness for the introduction of the new regulations in May this year. The Management Action The effectiveness of the revised constitution for the IGAB will be reviewed 6 months after the first meeting of the reconstituted information governance sub-group.	
Responsibility: Director of Public Health and Health Policy	Target date: 31 July 2018

Control objective2: An Information Governance Framework is in place and includes controls that support, compliance with the DPA, FOI, CG and PRA. **Associated risk of not achieving the control objective: Information may be shared, accessed inappropriately, or lost.**	**Medium**

Observation and risk

Information Governance have developed an Information Asset Register to record all information throughout NHS Lothian, Information is defined and managed in the register as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

NHS Lothian has a legal obligation to hold a register of all its information assets. If an individual or department has an information asset then it must be registered on the Information Asset Register.

Staff are required to complete a risk assessment for all information submitted to the Information Asset Register. As part of this each asset must be scored and a risk grade calculated. Information assets assigned a risk grade of 20-25 (very high) should, according to the guidance be reviewed each month to confirm that it is still required and is held securely. Information with a risk grade of high should be reviewed quarterly, medium every six months and low should be annually.

In July 2017, the Executive Director, Nursing, Midwifery and AHP's as NHS Lothian's Senior Information Risk Owner wrote to all asset owners asking them to review their information assets held and advise Information Governance of any changes to their asset holdings. It is expected that this will become an annual exercise.

However, there are no controls in place within Information Governance to ensure that asset owners are reviewing their information assets throughout the year and at the frequency dictated by risk grading. Without reviewing the security, management and relevance of information at the appropriate frequency, there is a risk that information may be shared, accessed inappropriately, lost or held when no longer required.

Recommendation

The Information Governance Team should agree with the IGWG and IGAB appropriate controls for ensuring that information assets held are reviewed according to their risk rating.

Management Response

On the 1 February 2018 the Executive Director, Nursing, Midwifery and AHP's wrote to all information asset owners, informing them of the actions required prior to the upcoming change in Data Protection Legislation.

Lists of registered information assets were provided and request made that the owners instruct their Information Asset Administrators to review their information assets held and

provide responses to additional questions. The Management Action Staff within the Information Governance Team will issue correspondence to information asset holders at intervals relevant to their risk rating, reminding then to review their information held.	
Responsibility: Information Governance and Security Manager	Target date: 31 July 2018

Control objective 3: Management monitors compliance with the Information Governance Framework and reviews performance against it.

We identified no significant Issues in relation to this control objective.

At each meeting, the IGWG is presented with three standard reports:

- FairWarning report, covering the previous 12 months and reporting on the number of incidents by medical staff of viewing their own or other records out with their clinical care responsibilities.

- IT Security report, providing information on blocked USB devices, internet activity and the threats presented and blocked from malware / viruses.

- Information Governance report, presenting data on FOI requests, subject access requests, training given & workshops held (including briefing sessions and LearnPro compliance), Information Asset Register forms & Caldicott applications, and Datix Incidents (including a list of those escalated to management and the Information Commissioners Office).

The three tabled reports are discussed between the meeting attendees. Discussions can include specific queries around the numbers provided or suggested amendments to how the information is presented. For example at the IGWG in July 2017, the Information Governance and Security Manager requested that the IT Security Report is updated to allow for comparison of information against previous months. They also requested the Subject Access Request Information in the Information Governance Report is updated to provide compliance information against the requests dealt with in less than 30 days as per the new GDPR requirements.

The current timeline for responding to subject access requests is 40 calendar days, which will be reduced to 30 days following GDPR implementation. For the three months covering July to September 2017, 51 requests received for the RIE, WGH, SJH and LCTC (6% of the total of 835) had breached the 40 day timeline, with 47% of these attributable to issues from the medical notes scanning project and delays receiving approval from consultants. It is noted that for the three months covering April 2017– June 2017, 27% of all subject access requests processed through the Medical Legal department were completed after 30 days (data for July-September was unavailable), indicating that some work is necessary to address the main causes for delays and meet with the GDPR requirement.

It is noted that no information is provided to the IGWG on Privacy Impact Assessments, which should be completed and submitted to the Information Governance Team for any new/change in service which utilises personal identifiable information. This is indicative of a relatively low completion rate of these forms. However this has been recognised by management and the review, update and relaunch of the PIA documentation is included within the GDPR action plan. Once done, this will be included in the Information Governance report. Although it is noted that submissions to the Information Asset Register includes information similar to that included in a Privacy Impact Assessment, with separate full assessment required for instances where a large amount of data is involved and Caldicott approval required.

Control objective 4: New and existing staff members receive training about Information Governance Policies and procedures. **Associated risk of not achieving the control objective: Staff may not be completely aware of their roles and responsibilities around information governance and how to ensure that information is subject to appropriate controls.**	**Medium**

Observation and risk

NHS Lothian has formal information governance training materials in place for all staff. This includes induction training for all new staff as part of the corporate induction process as well as ongoing training for all staff. The ongoing training is undertaken through all staff being required to complete the LearnPro e-learning module every two years.

The Information Governance Team also provides regular Information Governance Roadshows and briefing sessions across all NHS Lothian sites. These provide an overview of social media usage, IT security, confidentiality and the FairWarning system.

Overall, 90% of NHS Lothian staff are up-to-date with their Information Governance training. This figure includes the completion of LearnPro modules and any face-to-face training events, such as toolbox talks. This figure is above the 80% Board target for mandatory training.

However there are some areas within NHS Lothian where this has fallen below 80%, including:

- Edinburgh Partnership, Central Services (61%) (head count 57)
- Edinburgh Partnership, General Medical Services (53%) (head count 157)

Without being adequately trained, staff may not be completely aware of their roles and responsibilities around information governance and how to ensure that information is subject to appropriate controls.

Recommendation

Management should remind staff within the Edinburgh Partnership of the importance of keeping their mandatory training requirements up-to-date.

Management Response

Due to restructuring, staff have moved into new management areas. Edinburgh Partnership has also taken over management of several new GP Practices and is working to ensure that staff have completed and are compliant with all mandatory training, particularly new medical staff.

All managers of non-compliant staff were contacted on 16 February 2017 and requested to ensure staff have completed their LearnPro mandatory training by the end of March 2017.

The Management Action List of non-compliant staff is being reviewed and staff will be provided with support where necessary to complete their training.	
Responsibility: Primary Care Service Manager	Target date: 30 April 2018

Control objective 5: Actions arising from the submission of the Records Management Plan and Information Commissioners Audit are being addressed.

We identified no significant weaknesses in relation to this control objective.

Currently, the six elements within Records Management Plan the improvement model provided by The Keeper of the Records have not yet been taken forward into an action plan. This requires the reconvening of the NHS Lothian Public Records Management Plan Group to develop, who last met in April 2016. Although no meetings are currently scheduled.

However, it is noted that the Keeper of the Records of Scotland has indicated there are no elements within NHS Lothian's plan where there is a serious gap in provision, and has recommended that NHS Lothian should publish its agreed Plan as an example of good practice within the authority and the public sector.

There is 5-year timeframe for any work to take place, with a requirement to update the Keeper on progress annually. The Keeper published its NHS Lothian Assessment report in April 2017, with NHS Lothian expected to report progress to the Keeper by 31 March 2018.

The Information Commissioners Office undertook a follow-up audit in January 2017 and confirmed that the majority of actions from their original audit had been completed and evidenced. All outstanding issues have been addressed and the ICO is happy with the Board's progress. One action remains outstanding, however this cannot be progressed until such time that NHS Lothian's until new HR system is implemented and a means of tracking staff records established.

Control objective 6: The Healthcare Governance Committee receives regular reports about management actions to identify, investigate, report and address non-compliance with legal and regulatory responsibilities for Information Governance. **Associated risk of not achieving the control objective: Information governance matters do not receive adequate attention, time or scrutiny.**	**Low**

Observation and Risk

We identified no significant weaknesses in relation to regular reporting, however we have raised one finding in regards to the governance structure.

The Healthcare Governance Committee has overall ownership for information governance monitoring and scrutiny and has delegated responsibilities to the Information Governance Assurance Board (IGAB), which is a subcommittee and meets quarterly. To support the IGAB operationally there is also an Information Governance Working Group (IGWG), which meets quarterly, with minutes for this group provided to the IGAB.

The Healthcare Governance Committee is presented in September each year with an Information Governance Annual report. The report covers the period 1 April - 31 March and advises the Committee on the work carried out by the IGAB within the past year, including compliance with legal and regularity responsibilities.

The report presented to the Committee in September 2017 recommended that it acknowledge the upcoming changes in legislation for the General Data Protection Directive (GDPR), and the organisational requirement to prepare to comply on its enactment on 25th May 2018.

Also, the Committee is presented with the minutes of the IGAB on an exception basis.

Furthermore, the Healthcare Governance Committee in January 2018 approved an updated remit for the IGAB, also known as the Information Governance Subcommittee. As well as formalising the membership of the group, the remit has documented its key activities, which include:

- Agree and carry out a work plan which ensures that the subcommittee's activities do cover its assurance needs;
- Review the content of the Board's risk registers, and seek assurance that management have an adequate improvement plan in place to attend to any information governance risks in a timely manner;
- Monitor reports relating to information security and adverse event logs, and seek assurance that management are taking appropriate action, and
- Seek assurance that the organisation has a comprehensive understanding of all legal and regulatory requirements relating to information governance that it has to observe.

It will be the responsibility of this subcommittee to inform and advise the Healthcare

Governance Committee, other committees, and executive management of the outcome of its work. The Board's Caldicott Guardian will be routinely invited to attend meetings of the subcommittee.

The subcommittee shall prepare an annual report (for the year ending 31 March) to inform the Governance Statement in the format which the Audit & Risk Committee has agreed.

Given the broad remit of the Healthcare Governance Committee, and the delegation to sub-groups and working groups there is an increased risk that information governance matters do not receive adequate attention, time or scrutiny.

Recommendation

Management should review whether the current structure is best placed to provide scrutiny of Information Governance, in particular confirm the reporting lines between the sub-committee and the Healthcare Governance Committee to ensure that those lines are clearly communicated and issues can be escalated between the sub-committee and the Healthcare Governance Committee, and that ownership and accountability for information governance is understood and well defined.

Management Response

The revised constitution for the IGAB has been prepared to introduce a greater degree of governance over how NHS Lothian manages its information.

In addition to the annual report, minutes from the meetings of the IGAB will be routinely presented to the Healthcare Governance Committee.

The Management Action

Management will consider how information is being presented to the Healthcare Governance Committee. This will include approaching members of the Committee to receive opinion.

The IGAB will agree further controls whereby additional information (reports etc) is presented to the Committee as necessary.

Responsibility:	Target date:
Director of Public Health & Health Policy	31 July 2018

Appendix 1 - Definition of Ratings

Findings and management actions ratings

Finding Ratings	Definition
Critical	A fundamental failure or absence in the design or operating effectiveness of controls, which requires immediate attention
High	A key control failure has been identified which could be either due to a failure in the design or operating effectiveness. There are no compensating controls in place, and management should aim to implement controls within a calendar month of the review.
Medium	A control failure has been identified which could be either due to a failure in the design or operating effectiveness. Other controls in place partially mitigate the risk to the organisation, however management should look to implement controls to fully cover the risk identified.
Low	Minor non-compliance has been identified with the operating effectiveness of a control, however the design of the control is effective

Report ratings and overall assurance provided

Report Ratings	Definition	When Internal Audit will award this level
No assurance	The Board cannot take any assurance from the audit findings. There remains a significant amount of residual risk.	The controls are not adequately designed and / or operating effectively and immediate management action is required as there remains a significant amount of residual risk(for instance one Critical finding or a number of High findings)
Limited assurance	The Board can take some assurance from the systems of control in place to achieve the control objective, but there remains a significant amount of residual risk which requires action to be taken.	This may be used when: • There are known material weaknesses in key control areas. • It is known that there will have to be changes that are relevant to the control objective (e.g. due to a change in the law) and the impact has not been assessed and planned for. The controls are deficient in some aspects and require management action (for instance one 'high' finding and a number of other lower rated findings)
Moderate assurance	The Board can take reasonable assurance that controls upon which the organisation relies to achieve the control objective are in the main suitably designed and effectively applied. There remains a moderate amount of residual risk.	In most respects the "purpose" is being achieved. There are some areas where further action is required, and the residual risk is greater than "insignificant". The controls are largely effective and in most respects achieve their purpose with a limited number of findings which require management action (for instance a mix of 'medium' findings and 'low' findings)
Significant assurance	The Board can take reasonable assurance that the system(s) of control achieves or will achieve the control objective. There may be an insignificant amount of residual risk or none at all.	There is little evidence of system failure and the system appears to be robust and sustainable. The controls adequately mitigate the risk, or weaknesses are only minor (for instance a low number of findings which are all rated as 'low' or no findings)