Internal Audit

Information Governance – GDPR

July 2019

Internal Audit Assurance assessment:

Objective One	Objective Two	Objective Three
Significant Assurance	Significant Assurance	Significant Assurance

Timetable

Date closing meeting held: 19 July 2019

Date draft report issued: 30th July 2019

Date management comments received: 16th August 2019

Date Final report issued: 16th August 2019

Date presented to Audit and Risk Committee: 26th August 2019

Contents

1. Introduction

1.1 As part of the annual Internal Audit Plan for 2019-20, approved by the Audit and Risk Committee (ARC), we undertook a review of the General Data Protection Regulation (GDPR) and the controls in place at NHS Lothian to ensure NHS Lothian can demonstrate compliance with GDPR, alongside the Information Commissioners Office (ICO) 12 step model.

1.2 GDPR came into force on 25 May 2018 and all organisations, including the NHS, need to demonstrate compliance with the act. Failure to meet the Act's requirements could result in fines for NHS Lothian, alongside an impact on its reputation. NHS Lothian used the guidance prepared by the Information Commissioner's Office (ICO) and followed the 12 step requirements, working closely with other NHS boards and co-ordinating activities through the Information Governance & Security team managed by the Information Governance Manager.

Scope

1.3 The objective of the audit was to review the Board's self- assessment of its compliance with GDPR and the action plan established by NHS Lothian to ensure they identify and mitigate risk in respect of gaps and ensuring ongoing compliance. We considered evidence to support the Board's assessment of compliance, including design (policies and procedures) and operation of controls on a sample basis.

Acknowledgements

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

2. Executive Summary

Summary of Findings

2.1 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	NHS Lothian can demonstrate compliance with the ICO 12 GDPR steps and staff are aware of GDPR requirements.	Significant Assurance	-	-	-	-
2	NHS Lothian accurately documents the information assets it holds, processes Subject Access Requests and reports data breaches in line with GDPR requirements.	Significant Assurance	-	-	-	1
3	NHS Lothian keep updated with ICO guidance and incorporate this into action plans.	Significant Assurance	-	-	-	-
TOTAL			**-**	**-**	**-**	**1**

Conclusion

2.2 The area under review comprised 3 control objectives, of which 3 received Significant Assurance

2.3 The wider organisation was effectively notified about the required implementation of the new data protection guidance, and targeted training was provided to staff. There was effective planning and oversight to implement the process, with action plans put in place to ensure compliance with the ICO 12 steps, with each action assigned an owner required end date and evidence to demonstrate completion. NHS Lothian are represented on a Scottish-wide information governance group which covers data

protection, ensuring they are sighted on upcoming issues and best practice can be shared .

2.4 However, for one site, the Chalmers Centre, which processes some subject access requests (SARs), statistics are not being reported to committee and all expected documentation is not retained.

Main Findings

2.5 Staff within the organisation, and senior committees, were informed about the introduction of GDPR and its implications. As part of the implementation work, an action plan was provided to meetings of the Information Governance Working Group, with the action plan stating specific measures which would be used to test the effectiveness of the implementation.

2.6 In addition, staff received training specific to their needs. Those staff who required a detailed understanding received dedicated training from an external firm, as did staff tasked with dealing with subject access requests. Also, the Information Governance team provided roadshows on the topic in addition to the training available through the electronic system learnPro.

2.7 We identified the following area for improvement during the review:

2.7.1 Patients, or those acting on their behalf, can ask NHS Lothian for copies of information held on them: these are called subject access requests (SARs). Once a request has been received, NHS Lothian has to provide the information within the timeline stated by the guidance issued by the ICO. Statistics on SARs, which include the number of requests and the percentage that were complied with within the deadline, are provided to each quarterly meeting of the Information Governance Sub-Committee. However, there is no reporting of SAR statistics for the Chalmers Centre, which processes a small number of SAR in the year and from a review of a sample of 8 SARs for the Chalmers Centre, it was identified that not all relevant information relating to the SARs has been retained. While we recognise the Chalmers Centre is responsible for a smaller number of SARs (approximately 1.5% of the total population), it is still important that performance is monitored and documents are retained to ensure compliance.

2.8 Details of these findings are set out in the Management Action Plan.

3. Management Action Plan

Finding 1	
Control objective 2: NHS Lothian accurately documents the information assets it holds, processes Subject Access Requests and report data breaches in line with GDPR requirements. **Associated risk of not achieving the control objective: Subject access requests for the Chalmers Centre are not being reported to committee, and documentation held by the site is not comprehensive.**	**Low**

Observation and risk

Patients, or those acting on their behalf, can ask NHS Lothian for copies of information held on them. Once a request has been received, NHS Lothian has to provide the information within the timeline stated by the guidance issued by the Information Commissioner's Office (ICO). NHS Lothian will also, where appropriate, ask relevant clinicians to review medical records before they are issued in order to ensure that releasing any of the information will not cause harm to the patient, or identify any other person (other than clinical staff).

Currently requests are made under the Subject Access provisions of the Data Protection Act 2018 in line with the General Data Protection Regulation (GDPR). Before the introduction of the 2018 Act, NHS Lothian had 40 days to respond to a subject access request (SAR), but this has now been reduced to approximately 30 days.

SARs are processed at different NHS Lothian sites, including the Royal Infirmary Edinburgh (RIE) and the Chalmers Centre. The majority of SARs are processed at the RIE (98.5% of requests) with the remainder processed at the Chalmers Centre (1.5%). Statistics on SARs, which include the number of requests and percentage that were complied with within the deadline, are provided to each quarterly meeting of the Information Governance Sub-Committee. The statistics cover NHS Lothian acute sites, community, and directly managed GP practices.

Although it processes a lower number of SARs, our testing identified that there is no reporting of SAR statistics for the Chalmers Centre. In addition, from our sample of 24 SARs, 8 were for the Chalmers Centre and our testing showed that for these not all relevant information relating to the SARs has been retained:

- date stamps are not used for requests received by the Chalmers Centre
- copies of the covering letters sent to patients are not retained by the Chalmers Centre
- in 2 (25%) instances some dates were not stated in the monitoring spreadsheet: (i) the date casenotes were returned by the consultant; and (ii) the date casenotes were provided to the requester.

Although it processes a lower number of requests, if SAR statistics are not regularly reported for the Chalmers Centre to committee then there is an increased risk that performance issues are not noted and dealt with in a timely manner. Additionally, if documentation for SARs are

not retained or sufficient there is a risk that NHS Lothian will not be able to demonstrate compliance with the Data Protection Act.	
Recommendation Subject access request statistics for all parts of the organisation should be regularly reported to committee. Specifically, the statistics for the Chalmers Centre should be provided to the Information Governance Sub-Committee each quarter. Each NHS Lothian location that responds to subject access requests should retain documentation relating to each request, including the request letter (which has been date-stamped), the date information has been supplied to and received back from clinicians, and the letter provided to patients when notes are sent to them (also date-stamped). A monitoring spreadsheet should also be employed to record of all of this information.	
Management Response Agreed. The Management Action Chalmers Centre have agreed to provide statistics for the Information Governence Sub Committee Chalmers Centre to update local process in line with NHS Lothian Subject Access policy	
Responsibility: Information Governance Manager	Target date: 31 December 2019

4. 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 respects 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)

5. Appendix 2 – Staff involved, documentation, and testing performed

Staff Involved:

- Information Governance Manager
- Data Protection Manager
- Legal Services Manager, RIE eHealth Records
- Clerical Officer, RIE eHealth Records
- Business Manager, Chalmers Centre
- Team Manager, Chalmers Centre

Documentation reviewed:

- Subject access request monitoring spreadsheets
- Information Governance Sub-Committee minutes and reports
- GDPR action plan
- CMT briefing document and minute
- Emails to subject matter experts and training provided
- Information audit results
- Analysis of data processing activity within the organisation and templates
- Procedures for individuals' data rights, for patient consent, to identify new data processing and transfer of data internationally
- Systems in place to manage consent for children
- Information Commissioners' Office guidance on GDPR
- Data Protection Act 2018
- GDPR training materials for senior staff
- Approval of the DPO for primary care
- Datix report showing data protection issues for 2018 and 2019
- Data protection legislation – approval of additional funding by the CMT
- Information Governance Working Group incident log
- GDPR communication plan
- Review of evidence used to demonstrate GDPR compliance within the organisation – sample of 24 items of evidence
- Subject access requests – effective and timely statistical reporting to committee
- Subject access requests – sample of 24 requests
    - Confirmation of ID
    - Request letter, including date stamp
    - Casenotes supplied to clinician, where relevant, and returned
    - Issue of clinical information to requester
    - Information within documentation agrees to monitoring spreadsheet.