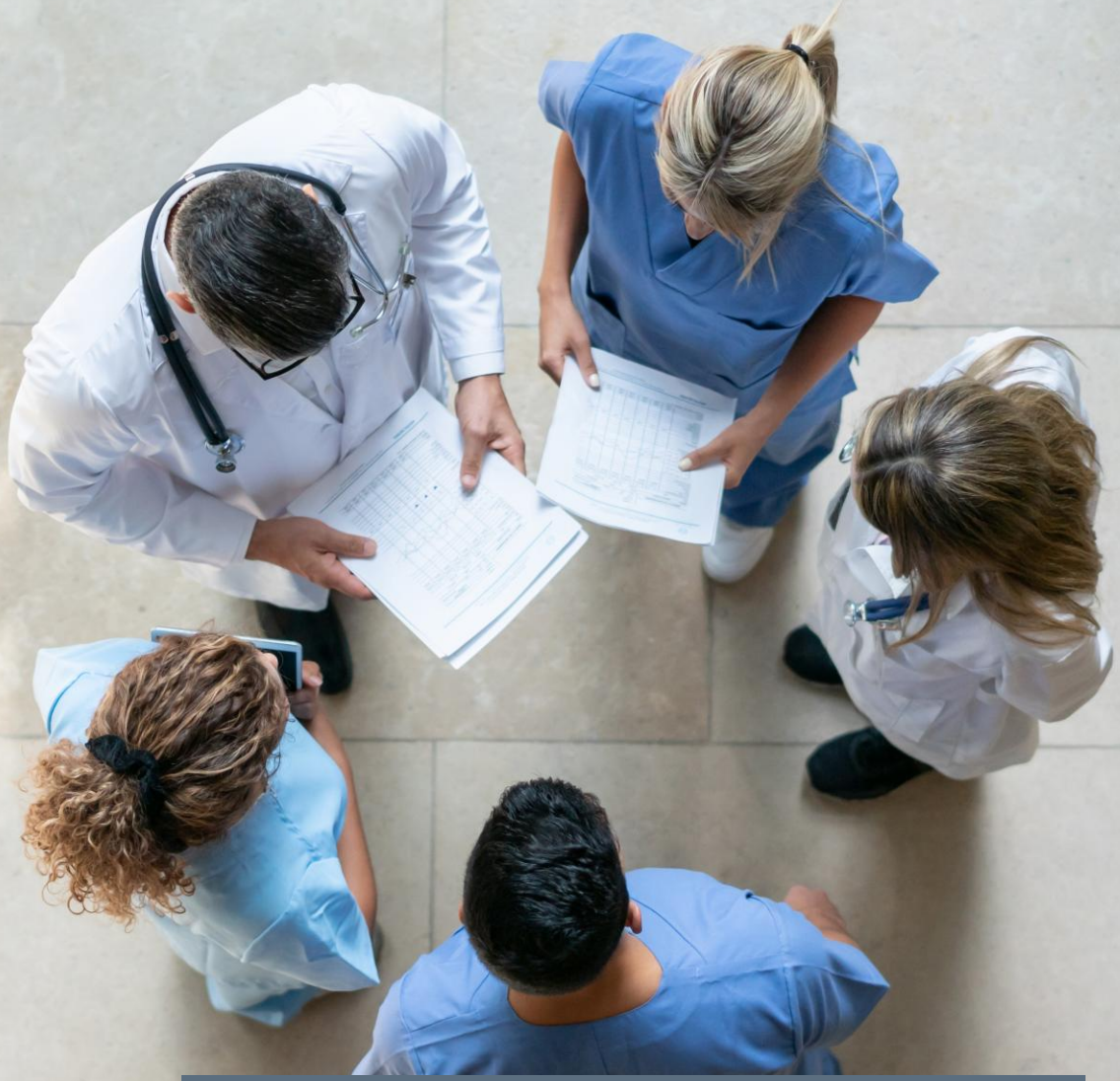
NHS Lothian

Information Governance

Internal Audit Report - Final

March 2026



Level of assurance:	
Design	Moderate
Effectiveness	Moderate

IDEAS | PEOPLE | TRUST

Contents

1. Executive Summary	3
2. Detailed Findings	7
3. Observations	21
4. Appendix I: Background	23
5. Appendix II: Definitions	26
6. Appendix III: Terms of Reference	27
7. Appendix IV: Staff interviewed	28
8. Appendix V: Responsibilities, limitations and conformance...	28

Distribution List		
For action	Tracey Gilles	Executive Medical Director and Caldicott Guardian
	David Stibbards	Director of Digital and IT
	Lisa Watson	Head of Health Records
	Tracey McKinley	Information Governance & Security Manager & Data Protection Officer
For information	Audit Committee	Members

Report Status	
IA delivery team:	Claire Robertson, Gemma MacLeod, Russell Richmond-McIntosh
Fieldwork performed:	12 January 2026 - 23 February 2026
Initial findings shared:	11 March 2026
Draft report issued:	19 March 2026
Management responses received:	26 March 2026
Final report issued:	26 March 2026

Executive Summary

Level of assurance: (see appendix II for definitions)		
Design	Moderate	Generally a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Moderate	Evidence of non compliance with some controls, that may put some of the system objectives at risk.

Summary of findings		# of agreed actions
H	0	0
M	5	7
L	2	3
Total number of findings: 7		

Background

It was agreed as part of the 2025-26 Internal Audit Plan that Internal Audit would conduct a review of the arrangements around Information Governance at NHS Lothian. Following an initial scoping meeting, it was agreed that this review would focus specifically on controls related to UK GDPR, Subject Access Requests (SARs) and Caldicott Principles.

Subsequent to the UK's departure from the European Union, UK-based organisations are subject to the UK GDPR (enshrined within the Data Protection Act 2018) for any data processing in the UK. However, the Health Board should be fully aware of the need to still apply the EU GDPR for any processing of EU based data subjects. For UK organisations, the changes are minimal, the UK GDPR almost mirrors the EU GDPR in full. The risks associated with non-compliance with UK and EU GDPR are significant, amounting to a maximum of £17.5 million (€20 million) or 4% of global turnover (whichever is greater), and associated reputational damage.

NHS Lothian processes personal data as part of:

1. Healthcare Services – concerning patients, including their medical records and treatment plan.
2. Operational Activities – involving current and former employees, recruitment applicants, and some special category data

Subject Access Requests (SARs) are a vital part of data protection, allowing individuals to access their personal data held by organisations. NHS Lothian is required to process SARs in accordance with the Data Protection Act 2018. This means they must respond to requests within one month, providing individuals with access to their personal data related to healthcare services or operational activities. NHS Lothian must ensure compliance with these regulations to protect individuals' privacy and maintain trust. Failure to comply can lead to significant penalties and reputational damage. In the last six months, NHS Lothian has moved from a paper-based system to an SAR portal.

The Caldicott Principles are guidelines designed to ensure the protection and confidentiality of patient information within healthcare settings. NHS Lothian, like other healthcare organisations, adheres to these principles to safeguard personal data. The principles emphasise the importance of justifying the purpose for using patient information, ensuring that only necessary data is accessed, and maintaining strict confidentiality. They also stress the need for transparency with patients about how their information is used and shared. By following the Caldicott Principles, NHS Lothian aims to uphold the highest standards of data protection and patient trust.

Purpose

The Information Governance Internal Audit aimed to provide assurance to management and the Audit and Risk Committee that the controls managing information governance are effective. This review considered processes around compliance with UK GDPR, Subject Access Requests and Caldicott Principles.

Conclusion

During the course of our review, we identified a total of seven findings, of which five were assessed as medium significance and two were assessed as low significance.

We have noted that there is a framework in place, designed to provide senior management and staff with instruction and guidance around information governance, while supporting legislative compliance.

A number of policies and procedures are documented and available to guide staff on their individual roles and responsibilities around information governance, with training also in place to ensure ongoing understanding and awareness. The introduction of a Training Strategy in October 2025 by information governance is a useful tool to ensure that training is appropriate for all staff groups and locations.

The Subject Access Request portal is operating effectively, with no issues noted in relation to the time take to respond to requests. With the 'audit' of the Portal by Information Governance noted as a useful exercise.

Applications to the Caldicott Guardian are subject to appropriate scrutiny and sign-off by the relevant individuals.

There are effective governance and oversight controls in place to ensure that operational performance is being routinely reported to the appropriate group.

The areas for improvement identified relate to documentation and guidance review and update, training compliance, ROPA update, ongoing operational effectiveness of the SAR Portal, Caldicott application review and formal governance and reporting arrangements.

We are able to give a moderate level of assurance over the design and operational effectiveness of controls in place around information governance.

Executive Summary

SUMMARY OF GOOD PRACTICE

We noted a number of areas of good practice being demonstrated at the organisation in relation to Information Governance. These include:

- Organisational charts have been developed to formalise the Board's reporting and oversight responsibilities around information governance. These detail the high-level reporting arrangements in place, alongside the departmental roles and responsibilities.
- A number of governance groups, with varying responsibilities for information governance are in place and their specific roles around Information Governance documented in Terms of Reference.
- Staff are able to access a dedicated information governance intranet site to view relevant documentation, request training, or raise issues around potential data breaches.
- NHS Scotland has developed a Once for Scotland approach to core mandatory learning requirements which must be undertaken by all staff. The Information Governance modules are completed through the organisation's TURAS software and repeated every 2 years by all staff. The Information Governance module includes IT Security, Data Protection Policy and Records Management.
- In October 2025, the Information Governance Team produced an Information Governance Training Strategy, which has identified the varying learning needs across NHS Lothian for Information Governance and Data Protection. This includes NHS Lothian's core mandatory learning requirements, alongside other more specific training and advisory arrangements.
- A training log is in place within Information Governance which records all training that has been provided to GP surgeries and wider Board services and departments. The training provided varies according to need and includes Fairwarning, redaction, SAR/disclosure, DPIAs & DSAs, and general awareness.
- The Information Governance Team have in place an Action Plan, which includes ensuring that NHS Lothian is ensuring awareness of responsibilities regarding data protection legislation. This is routinely reviewed and updated by the Team.
- A number of policies and procedures are in place and accessible through the Information Governance intranet pages and Policy Online. These are subject to formal review procedures to ensure that they remain up-to-date and aligned with relevant legislation.
- Guidance is available to advise staff on the importance of maintaining an accurate and up-to-date Record of Processing Activity (ROPA), noting that this is a core requirement under UK GDPR and an essential part of demonstrating accountability in how NHS Lothian manages personal data. A ROPA is in place and maintained by Information Governance.
- Privacy notices are published through the Board's public website and intranet. Arrangements are in place through the Information Governance Action Plan for their routine review and update where necessary. Information Governance also advise GP Practices and Medical Centres to ensure that their own notices are accurate and up-to-date.
- A Personal Data Breach Flowchart is in place to advise staff on how incidents involving personal data breaches must be handled. All breaches and incidents are assessed by Information Governance to determine any corrective actions and whether notification should be made to the Information Commissioners Office.
- Data Protection Impact Assessment (DPIA) guidance is in place and available through the Information Governance Intranet Pages. DPIAs are completed using a national template and once approved, recorded in the ROPA.
- Subject Access Requests are being processed appropriately through the online SARs portal. Monitoring controls are in place to identify and escalate requests that are at risk of breaching the defined timescales.
- Information Governance have caried out an audit of the Subject Access Portal to evaluate how it is configured and assists with compliance with Data Protection Legislation.
- Caldicott policies, protocols and operational processes are clearly documented. With additional advice provided through the Board's Data Protection policy and Policy on Confidentiality of Personal Health Information.
- In addition to the Caldicott applications received through the office of the NHS Lothian Caldicott Guardian, delegated authority has also been granted by them to NHS Lothian Research & Development for the review and approval of Caldicott applications. Records of all applications are maintained.
- Appropriate scrutiny is being applied to monitoring performance through established governance groups.

Executive Summary

SUMMARY FINDINGS

Notwithstanding the areas of good practice noted, we have also identified areas where further improvements can be made, the most significant of which are summarised below:

- **Staff Training** - The completion of the mandatory LearnPro Information Governance Module through the Turas platform, is below the Board's 90-95% target. Completion of the essential Managing Information Assets Module by Information Asset Owners and Information Asset Administrators has also been noted as low.
- **Record of Processing Activity** – Our review of the ROPA found that there are a total of 259 agreements marked as active; of these, 88 are recorded as under review dating from 2012 to 2024. We also noted that the lawful basis for processing is not recorded in the ROPA.
- **Caldicott Guidance** - The Confidentiality Policy does not include the current Caldicott Guardian for NHS Lothian. Both the Confidentiality Policy and Caldicott Website do not record all 8 Caldicott Principles, as defined by the National Data Guardian for Health and Social Care and the UK Caldicott Guardian Council. The Caldicott Manual available through the Caldicott Guardian intranet page is out of date and is now available online only through the UK Caldicott Guardian Council website.
- **Caldicott Principles - Retentions of Personal Data** - No processes are currently in place to ensure that personal identifiable data collated during projects is deleted by the destruction date and as per the Caldicott form.
- **Policy Review & Update** – The Confidentiality Policy, Processing Access Request Procedure and Subject Access Requests – Staff Files Process have passed their review dates. We also noted that there are no model Caldicott Applications accessible through the Caldicott intranet site.

Detailed Findings

Detailed Findings

Risk: Failure to clearly define and assign ownership for information governance could result in inconsistent practices and non-compliance with data protection requirements, leading to financial penalties and reputational damage.

Finding 1 - Staff Training	Type
NHS Lothian has formal information governance training material in place for all staff. All new starts are provided with the NHS Lothian induction training and materials. To support this an onboarding roadmap and checklist have been prepared to ensure that the mandatory eLearning requirements are met from the outset, which includes Information Governance training. Thereafter, staff are expected to complete this mandatory training module every 24 months, which includes IT Security, Data Protection Policy and Records Management. NHS Scotland has this year developed a Once for Scotland approach to core mandatory learning requirements which must be undertaken by all new employees during their induction. The Information Governance modules are completed through the organisation's Turas software and must now be repeated annually by all staff. There are two modules that should be completed, these are Cyber Security and Safe Information Handling. As at December 2025, the compliance rate for completion of the Information Governance module is 75.9%, Lothian-Wide. While NHS Scotland does not publish a single national Turas training completion target, NHS Lothian has determined that a 90%-95% completion target is to be achieved for all core mandatory training. This has been discussed by the Information Governance Working Group at its most recent meeting in January 2026, however no action has yet been taken to highlight to the appropriate group the low compliance rate and any actions necessary to increase it. In addition to the core mandatory training for all staff, staff with responsibilities as Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are required to complete the essential Learnpro Managing Information Assets Module available through Turas. As advised in the routine emails prepared and sent out to IAOs. There are 29 IAOs and 1,764 active IAAs across NHS Lothian, overseeing 2,085 information assets. However, it has been advised by Information Governance that only 12 members of staff have completed the module.	Effectiveness 
Implication	**Significance**
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.	Medium

Detailed Findings

Risk: Failure to clearly define and assign ownership for information governance could result in inconsistent practices and non-compliance with data protection requirements, leading to financial penalties and reputational damage.

Finding 1 - Staff Training			Type
Recommendations	Action owner	Management response	Completion date
The Information Governance Working Group should agree on the appropriate means of reporting mandatory training compliance and thereafter management should remind staff of the importance of keeping their mandatory training requirements up-to-date.	Director of People & Culture	The mandatory training statistics are supplied by Human Resources. There is currently a change of system from LearnPro to TURAS therefore these stats maybe lower than expected. 74%, number consistently available. The Information Governance Working Group may support staff promotion in the completion of staff modules, but Staff Governance and Departmental managers have responsibility of staff engagement.	TBC
Completion of the Managing Information Assets Module should be raised with the Board's Senior Information Risk Officer and instruction given to IAOs and IAAs to complete this. Monitoring controls should also be introduced to ensure compliance.	Director of Public Health & SIRO and Information Governance & Security Manager	Information Governance & Security Manager will draft response from Senior Information Risk Office to engage with Information Asset Owners'/Information Asset Administrator to instruct completion of this module.	May 2026

Detailed Findings

Risk: Non-compliance with UK GDPR requirements, particularly around accountability and lawful processing, can lead to significant fines and erosion of public trust.

Finding 2 - Record of Processing Agreement	Type
Guidance is in place to advise staff on the importance of maintaining an accurate and up-to-date ROPA, noting that this is a core requirement under UK GDPR and an essential part of demonstrating accountability in how NHS Lothian manages personal data. The ROPA maintained by Information Governance was obtained and reviewed. This contains five worksheets, as below: • All Active Agreements • Closed Agreements • DPIA • Intra-Scotland Sharing • National DPIAs • GPs The ROPA clearly states where applicable any Joint Controller Relationships and third-party data processor relationships. Lawful bases for processing activities are determined through the completion of Data Processing Agreements, Data Protection Impact Assessments and Data Sharing Agreements. Column C of the ROPA spreadsheet records all third parties to which the agreement applies. There are a total of 259 agreements marked as active. Of these, 88 are recorded as under review dating from 2012 to 2024. With the majority dating as far back as 2019 (14 agreements), 2021 (28) and 2022 (22). We were advised by Information Governance staff that documents under review are the ones they are actively seeking confirmation from the IAO/Director that these are currently in place/closed/replaced/updated. Once they have confirmed these will be closed or updated on the ROPA, with a date of review then added. This task has been included in the Information Governance Action Plan. It was also noted that 17 active agreements have no review date assigned to them. We also noted that whilst lawful basis is considered as part of the completion of Data Processing Agreements, Data Protection Impact Assessments and Data Sharing Agreements, the lawful basis is not recorded as a field in the ROPA, which we would expect in line with best practice.	Design and Effectiveness
Implication	**Significance**
Out-of-date data processing or data sharing agreements may expose the Board to legal, security, and accountability risks because personal data may be handled without current, compliant controls or clearly defined responsibilities.	Medium

Detailed Findings

Risk: Non-compliance with UK GDPR requirements, particularly around accountability and lawful processing, can lead to significant fines and erosion of public trust.

Finding 3 - Record of Processing Agreement			Type
Recommendations	Action owner	Management response	Completion date
Management should ensure that all agreements are reviewed by the target date recorded in the Information Governance action Plan (June 2026). Thereafter, the ROPA should be updated with a review date for each active agreement to ensure ongoing relevance.	IG&S Manager and IAO's	All IAO's have previously been prompted to complete this task but the Information Governance & Security Manager will write to all IAO's to highlight this action is still outstanding and must be actioned. The IAO are responsible for agreements in their areas of responsibility.	June 2026
We recommend that a field is added to the ROPA to capture the lawful basis for processing.	Information Governance & Security Manager	Lawful basis is already recorded in the DPIA for each record of processing, but this addition can be easily added.	June 2026

Detailed Findings

Risk: Failure to incorporate Caldicott Principles into everyday practices may lead to inappropriate sharing of patient data and breaches of confidentiality, damaging patient trust.

Finding 3 - Caldicott Guidance	Type
Information Governance have two policies that include specific reference to the Board's Caldicott responsibilities. The Data Protection Policy records that NHS Lothian will observe the Caldicott Principles and ensure that there is a nominated Caldicott Guardian. In Conjunction with the Data Protection Legislation, NHS Lothian will apply the Principles of Caldicott, IT Security, Information Sharing, Confidentiality, Social Media, and Records Management, as defined in their supporting policies and protocols to meet the Information Governance standards as prescribed by Scottish Government. The Policy advises that the Executive Medical Director and Caldicott Guardian, is the named executive director on the Board with responsibility for Information Governance. The Policy on Confidentiality of Personal Health Information has recorded that staff must act in accordance with the six Caldicott Principles on best practice on the use of patient identifiable information. And that staff should only be carrying patient identifiable material on any device with the explicit permission of the Caldicott Guardian. According to the Policy, The Caldicott Review proposed six general principles that health and social care organisations should adopt when reviewing their use of client information. However, the NHS Lothian Caldicott intranet page refers to an additional 7th Principle which is not included in the Confidentiality Policy – 'The duty to share information can be as important as the duty to protect patient confidentiality - Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies'. Furthermore, the National Data Guardian for Health and Social Care has advised of an additional 8th Principle, which is not referenced in the Confidentiality Policy or on the Caldicott intranet page, which is: *'Inform patients and service users about how their confidential information is used*. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information.' Also, the Confidentiality Policy has recorded that corporate responsibility lies with the Director of Public Health and Health Policy and states that they are NHS Lothian's Caldicott Guardian; it is actually the Board's Executive Medical Director who is the nominated Caldicott Guardian. A Manual for Caldicott Guardians was produced by the UK Caldicott Guardian Council in 2017 and is available through the Caldicott Intranet site. It is also noted that the Council have since amended it's manual and made this available online only. With the 2017 now superseded by the online version.	Design
Implication	**Significance**
If the Board has not ensured that Caldicott guidance is complete, up to date, and clearly identifies the nominated Caldicott Guardian, it creates a significant governance and information-handling risk. There is a risk that this will weaken oversight of how personal and confidential information is used, shared, and protected.	Medium

Detailed Findings

Risk: Failure to incorporate Caldicott Principles into everyday practices may lead to inappropriate sharing of patient data and breaches of confidentiality, damaging patient trust.

Finding 5 - Caldicott Guidance			Type
Recommendations	Action owner	Management response	Completion date
The Confidentiality Policy should be updated to include the details of the Board's current Caldicott Guardian, which is the NHS Lothian Executive Medical Director.	Information Governance & Medical Director	The Policy will be reviewed and updated	End June 2026
The NHS Lothian Caldicott Guardian intranet page, Confidentiality Policy and associated Caldicott application forms should be updated to make reference to the 8 Caldicott Principles as defined by the National Data Guardian for Health and Social Care and the UK Caldicott Guardian Council.	Information Governance & Security Manager	Information Governance & Security Manager will work with the Calicott Administrator to update the Caldicott Guardian intranet page and application forms. As outlined the Confidentiality Policy sits with the Associate Director of Nursing	April 2026
The 2017 Caldicott Manual should be removed from the website and a link instead added to take users to the online version available through the UK Caldicott Guardian Council website.	Information Governance & Security Manager	Information Governance & Security Manager will work with the Calicott Administrator to update	Complete - 18/03/2026

Detailed Findings

Risk: Failure to incorporate Caldicott Principles into everyday practices may lead to inappropriate sharing of patient data and breaches of confidentiality, damaging patient trust.

.

Finding 4 - Caldicott Principles - Retentions of Personal Data			Type
Data destruction dates are included in the Caldicott forms. According to the form a checking system should be in place within the Caldicott Guardian's office where a sample of applications are audited to ensure data has been deleted at the end of the project. All applicants are advised to expect to be asked to evidence deletion. However, we have been advised by the Caldicott Support Officer that this is not currently done, and it was noted that from a sample of Caldicott applications tested, one application (from 7) had a destruction date of 12 June 2025, with no evidence in place to indicate that the project had concluded and person identifiable data deleted (No. 25102).			Effectiveness
Implication			**Significance**
If projects approved by the Caldicott Guardian are not routinely confirmed as closed and associated patient identifiable information is not deleted, NHS Lothian may face a significant confidentiality, compliance and data-retention risk.			Medium
Recommendations	**Action owner**	**Management response**	**Completion date**
A formal audit process for checking a sample of applications should be instated. Guidance should be documented on the frequency of checks, who is responsible for completing them, the sample sizes which will be used, and the process for following up on any exceptions.	Executive Medical Director and Caldicott Guardian	The Information Governance & Security Manager will assist the Caldicott Administrator to development of a process to review applications. This can be added to the Caldicott Guardian Reports meeting	June 2026

Detailed Findings

Risk: Outdated, inadequate, or poorly communicated IG policies and procedures may cause staff to overlook key obligations, increasing the likelihood of breaches.

Finding 5 - Policy Review and Update	Type
The Board have in place a number of policies and procedures to guide staff on their roles and responsibilities in ensuring that patient identifiable information is being managed appropriately and in line with current legislation and statutory requirements. Key policies are being routinely reviewed by the Board's Policy Advisory Group to ensure that these remain in date and compliant, sample testing has noted that a comprehensive review of policies took place last year, which included the following: • Data protection Policy • Subject Access Policy • Digital IT Security Policy • Records Management Policy • Information Risk Management Policy • Data Access for Research Policy • Warning and Alerts Policy Local arrangements are also in place to ensure the procedural documentation is also subject to routine review. While most Policies selected for review were found to be in date, clear and aligned with statutory requirements and best practice guidance, alongside the authors, owner and approvers clearly recorded; three policy and procedural documents were noted to have passed their review dates: • The Confidentiality Policy has a review date of April 2021 • The Processing Access Requests Procedure has a review date of June 2025 • The Subject Access Requests - Staff Files Process has a review date of June 2025 Additional analysis was completed on the content of the Caldicott intranet site to confirm that there was sufficient instruction provided. The Caldicott main page and additional linked page clearly states the principles that should be considered when submitting a Caldicott application, alongside frequently asked questions. However, while there are contact details, there are no model applications for reference and guidance when completing Caldicott application forms, despite there being a link to access them.	Design
Implication	**Significance**
The organisation is exposed to avoidable legal, security, and operational risks because staff are not being guided by current data protection requirements or best practice.	Medium

Detailed Findings

Risk: There may not be effective oversight to ensure compliance with the changes, leading to reputational damage and legal action against NHS Lothian.

Finding 5 - Policy Review and Update			Type
Recommendations	Action owner	Management response	Completion date
It is recommended that the Confidentiality Policy is reviewed and once approved published through the relevant sites. The Processing Access Requests Procedure, SAR – Staff Files process and Stored Information – SAR Portal SOP should also be reviewed.	Information Governance & Medical Director Information Governance & Security Manager	The Confidentiality Policy will be reviewed and updated The Processing Access Requests Procedure has been removed as added to intranet in error. Replaced with HRECS/PP/27 & HRECS/PP/28	June 2026 Complete – 17/03/2026
To ensure consistency across the policies and guidance documents, the Confidentiality Policy document should be updated to record author/owners and review date.	Information Governance & Medical Director	The Confidentiality Policy will be reviewed and updated	June 2026
To ensure that staff are able to complete Caldicott applications effectively and accurately, it is recommended that model applications are selected and made available through the Caldicott intranet site.	Information Governance & Medical Director	The Information Governance & Security Manager will work with the Caldicott Administrator to complete a cohort of model applications are held on the Caldicott intranet site for reference of applicants.	TBC

Detailed Findings

Risk: Failure to accurately log, manage, and disclose information in response to SARs within statutory timeframes could result in regulatory scrutiny, enforcement action, and reputational harm.

Finding 6 - Subject Access Requests	Type
In September 2025, NHS Lothian Information Governance Team carried out an audit of the Subject Access Portal. The Subject Access Request Portal has been Live in NHS Lothian since 31st March 2025, supporting streamlining applications and administration of the Data Protection Act. NHS Lothian Data Protection Officer public phone line had received several enquiries from the public about the use of the system, and therefore an audit was commissioned to support service and compliance with the Data Protection Act and ensure that NHS Lothian's Information Commissioner Office audit mandatory requirements are maintained. The scope and objective of the audit was to evaluate how the NHS Lothian SAR Portal is configured and assists compliance with Data Protection Legislation. This audit allowed NHS Lothian to assess compliance with NHS Information Governance standards and UK data protection legislation, including: UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Access to Health Records Act 1990 (for deceased patients) ICO guidance on SARs NHS Lothian policies and SOPs A random selection of applications from June 2025, and August 2025 totalling 200 SAR applications were reviewed. A total of 11 findings were identified and reported to the SAR Team within Health Records with recommended actions to address them. On 12 March 2026, Information Governance reviewed the updates and amendments carried out by the Health Records SAR Team and have concluded that they have addressed the audit recommendations. Some additional processes and actions have been added to the audit report and the Head of Health Records will review them in two months and on a regular basis thereafter.	Design and effectiveness 
Implication	**Significance**
Issues with Subject Access Requests may lead to delays, incomplete disclosures, privacy risks, and an increased administrative burden for the Board, affecting patient trust, legal compliance, and the quality of care.	Low

Recommendations	Action owner	Management response	Completion date
It is recommended that management ensure that the review date for the additional processes is adhered to and an ongoing schedule of review implemented.	Head of Health Records and IG&S Manager	The Head of Health Records and IG&S Manager will ensure a plan and implementation of process is in place for regular review of SAR process	September 2026

Detailed Findings

Risk: Insufficient oversight or inadequate performance reporting could mask noncompliance trends or repeated issues, leading to unresolved risks and potential regulatory action.

Finding 7 - Governance and Oversight	Type
It is important that there is a suitable level of oversight of Information Governance performance in order to identify and address any risks or potential issues. The March 2025 Information Governance Annual Report to the Healthcare Governance Committee has noted that the Digital Portfolio Group and the Information Governance Working Group provide compliance assurance oversight, with escalations to the Executive Medical Director (and Caldicott Guardian), the Executive Director of Public Health and Health Policy (and SIRO) and the Director of Digital and IT. While this has been confirmed for the Information Governance Working Group, we have noted that The Digital Oversight Board is currently under review and reestablishment as the Digital Portfolio Group (DPG) by the new Director of Digital and IT. During this period compliance monitoring arrangements at this level by the Digital Executive team and Free-standing meeting with Director of Digital, Executive Medical Director (Caldicott Guardian) and Executive Director of Public Health and Health Policy (SIRO). The Terms of Reference for the DPG notes that it will be directly supported in the area of information governance, management and security operations by the Information Governance Working Group (IGWG). The DPG will, once established, receive quarterly reports from the IGWG.	Design and Effectiveness

Implication	Significance
When information governance activities, issues, and performance are not fully or consistently reported into the Board's governance groups, the organisation loses essential oversight of how personal data is being managed. This creates a material risk of non-compliance with data protection legislation, Caldicott principles, and internal IG policies	Low

Recommendations	Action owner	Management response	Completion date
The Digital Oversight Board should be reestablished as the Digital Portfolio Group and formal compliance reporting arrangements from the IGWG put in place.	Director of Digital	The Director of Digital will reestablish the Digital Portfolio Group and invite the IG&S Manager to give compliance report.	May 2026

Appendices

Appendix I: Background

It was agreed as part of the 2025-26 Internal Audit Plan that Internal Audit would conduct a review of the arrangements around Information Governance at NHS Lothian. Following an initial scoping meeting, it was agreed that this review would focus specifically on controls related to UK GDPR, Subject Access Requests (SARs) and Caldicott Principles.

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

A formal Data Protection Policy is in place, alongside a number of other policies and procedures which provide guidance to all staff in the implementation of effective information governance. These include arrangements that promote compliance with the Data Protection Act, UK GDPR, Caldicott Guardian and Subject Access Requests legislation. All information governance policies and procedures are easily accessible to all staff via a number of information governance and Caldicott Guardian webpages.

Roles and responsibilities for information governance are clearly documented through the relevant terms of reference with an Information Governance Working Group (IGWG) established to ensure that operational compliance requirements are being monitored, reported and adhered to. An organisational chart shows how the Information Governance function fits into the overall NHS Lothian structure and documents the various Board Committees, governance groups and assurance providers that provide the structure for Compliance Reporting:

- The Healthcare Governance Committee receives an annual Information Governance Report
- The Audit and Risk Committee receives an annual Cyber Risk Paper.
- The Policy Approval Group is responsible for approving/updating the relevant Organisational Policies as required
- The Digital Oversight Board receives Highlight and Compliance Reports every two months.
- The Information Governance Working Group receives quarterly compliance reports and advises on policy and guidance.

Additional compliance groups, include in the organisation chart are:

- The Network and Information Systems Regulations (NISR)
- External Audit
- Information Commissioners Office (ICO)
- Internal Audit

The IGWG is presented wither several reports at each of its meetings, advising group members on a number of aspects of information governance. These include IT security, inappropriate access and subject access requests. All requests received through the new subject access request portal 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.

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. In addition, the Information Governance Team provides regular training across the organisation to address specific training requirements and requests and they have developed a comprehensive training strategy to identify the various learning needs across NHS Lothian.

At an operational level, all NHS Lothian staff are able to access the Information Governance intranet pages to contact the Team; refer to guidance, information, training and support materials; and access the various policies and forms. A separate Intranet page is in place for staff to understand the role of the Caldicott Guardian, understand the principles behind the use of patient-identifiable information and obtain approval

The processing of Caldicott Guardian information access requests is controlled, with all requests approved by either the Board's Caldicott Guardian, or individuals with appropriate delegated authority to do so.

Guidance is in place to advise staff on the importance of maintaining an accurate and up-to-date ROPA, noting that this is a core requirement under UK GDPR and an essential part of demonstrating accountability in how NHS Lothian manages personal data.

NHS Lothian has in place a SAR portal where all requests are logged and automatically assigned to staff. Once a request has been allocated staff will in the first instance check that all necessary supporting document are supplied, such as ID and proof of address, proof of authorisation if on behalf of a patient. There are checklists built into the portal for tracking progress against requests. In September 2025, NHS Lothian Information Governance Team carried out an audit of the Subject Access Portal; a random selection of applications from June 2025, and August 2025 totalling 200 SAR applications were reviewed.

Appendix II: Definitions

Level of assurance	Design of internal control framework		Operational effectiveness of controls	
	Findings from review	Design opinion	Findings from review	Effectiveness opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

Appendix III: Terms of reference

Extract from terms of reference
Purpose
The Information Governance Internal Audit was to provide assurance to management and the Audit and Risk Committee that the controls managing information governance are effective. This review considered processes around compliance with UK GDPR, Subject Access Requests and Caldicott Principles.
Key risks
• Failure to clearly define and assign ownership for information governance could result in inconsistent practices and non-compliance with data protection requirements, leading to financial penalties and reputational damage. • Outdated, inadequate, or poorly communicated policies and procedures may cause staff to overlook key information governance obligations, increasing the likelihood of breaches. • Non-compliance with UK GDPR requirements, particularly around accountability and lawful processing, can lead to significant fines and erosion of public trust. • Failure to accurately log, manage, and disclose information in response to SARs within statutory timeframes could result in regulatory scrutiny, enforcement action, and reputational harm. • Failure to incorporate Caldicott Principles into everyday practices may lead to inappropriate sharing of patient data and breaches of confidentiality, damaging patient trust. • Insufficient oversight or inadequate performance reporting could mask non-compliance trends or repeated issues, leading to unresolved risks and potential regulatory action.
Exclusions
The scope of the review was limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review. Our review will not provide assurance over all aspects of facilities service payments. This review did not cover Information Security which was the subject of previous internal audit coverage. We also note that NHS Lothian have been subject to an NIS (Network and Information Systems) audit. Where sample testing is undertaken, our findings and conclusions will be limited to the sample tested only. Please note that there is a risk that our findings and conclusions based on the sample may differ from the findings and conclusions we would reach if we tested the entire population from which the sample is taken.

Appendix IV: Staff interviewed

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.		
Tracey McKinley	Information Governance & Security Manager and Data Protection Officer	Key Contact
Elaine Downie	Interim Information Governance & Security Manager	Interviewee
Lisa Watson	Head of Health Records	Interviewee
Darren Poole	Information Governance Project Manager	Interviewee
Donna Weatherhead	Information Governance Project Officer	Interviewee
Neil Joshi	Health Records Manager	Interviewee
Graeme Allan	Health Records Assistant Manager	Interviewee
Denise Foley	Caldicott Support Officer	Interviewee
Pamela Linkstead	eResearch Lead	Interviewee
Pavlena Yaneva	R&D Information Governance Lead	Interviewee

Appendix V: Responsibilities, limitations and conformance with the Global Internal Audit Standards

Management responsibilities

The Board is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The Board is responsible for ensuring the internal audit function has:

- The support of the Company's management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.
- The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Company.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the Company in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

Limitations

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

Conformance with the Global Internal Audit Standards This engagement has been conducted in accordance with the Institute of Internal Auditors' Global Internal Audit Standards.

FOR MORE INFORMATION:

Claire Robertson, Head of Risk Advisory Services - Scotland

07583 237 579
Claire.robertson@bdo.co.uk

Freedom of Information

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 ("the Act"), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure, and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.

Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

www.bdo.co.uk