Liverpool University Hospitals NHS Foundation Trust

Data protection audit report

February 2025

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOI 2000) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

The purpose of the audit is to provide the Information Commissioner and Liverpool University Hospitals NHS Foundation Trust ('the Trust') with an independent assurance of the extent to which the Trust, within the scope of this agreed audit, is complying with data protection and Freedom of Information (FOI) legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust's processing of personal data and FOI practices. The scope may take into account any data protection and FOI issues or risks which are specific to the Trust, identified from ICO intelligence or the Trust's own concerns, or any data protection

and FOI issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of the Trust, the nature and extent of the Trust's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the Trust.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Information and Cyber Security	The organisation has an effective Information Security Management System (ISMS) in place with appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of personal data and protect information processing systems and facilities from cyber security threats.
Freedom of Information	The extent to which FOI/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

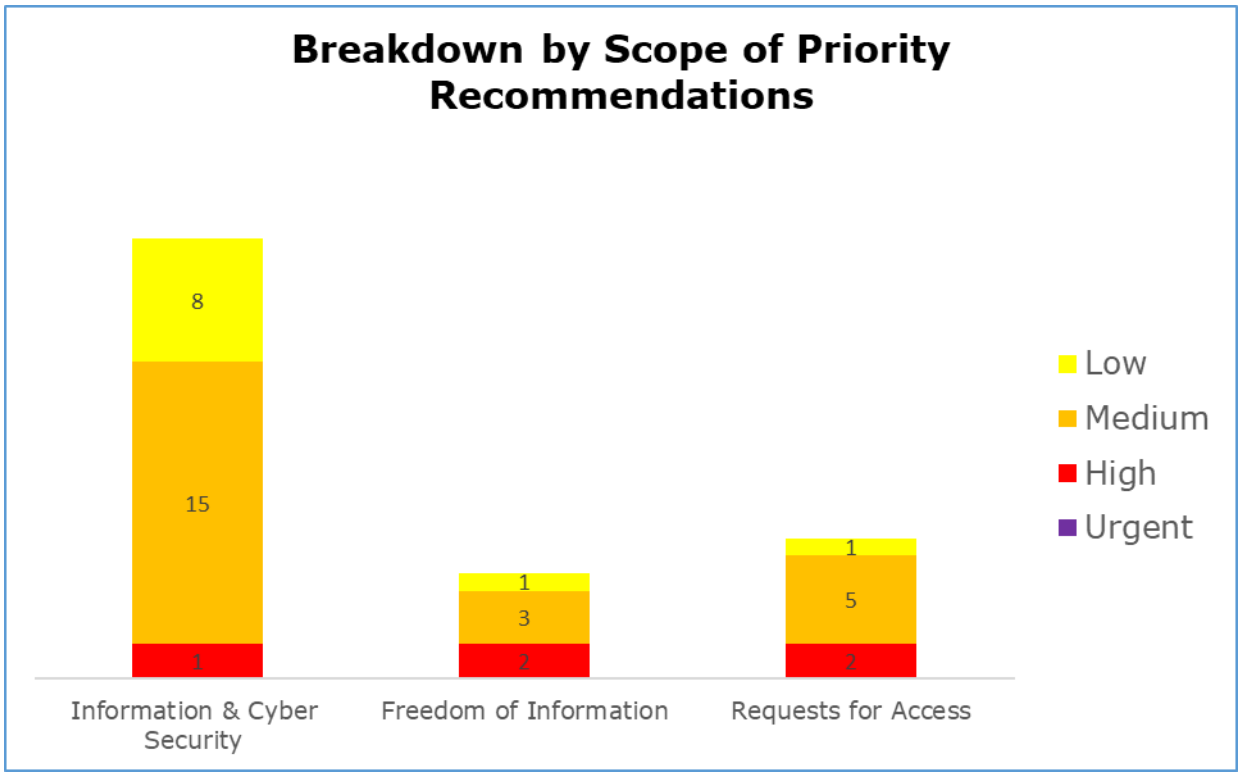
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address.

The ratings are assigned based upon the ICO's assessment of the risks involved. the Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Information and Cyber Security	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Requests for Access	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

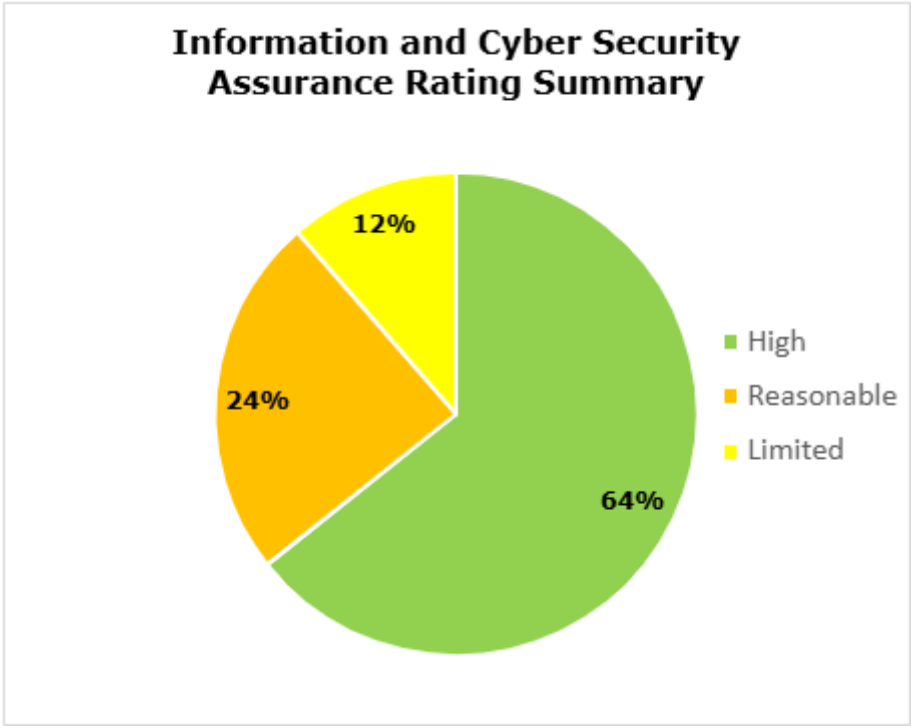
Priority Recommendations



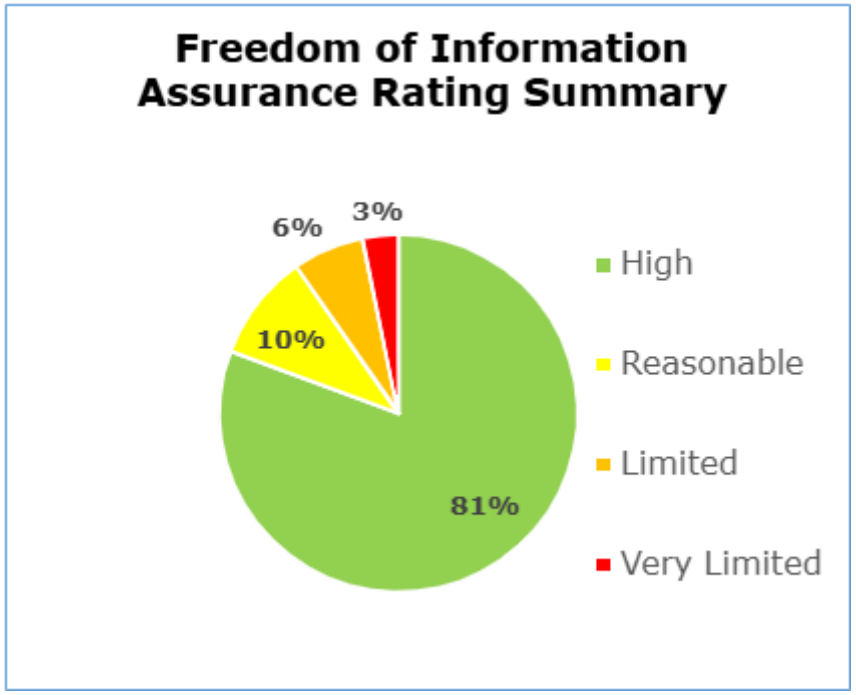
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Information and Cyber Security has no urgent, one high, 15 medium and eight low priority recommendations
- Freedom of Information has no urgent, two high, three medium and one low priority recommendations
- Requests for Access has no urgent, two high, five medium and one low priority recommendations

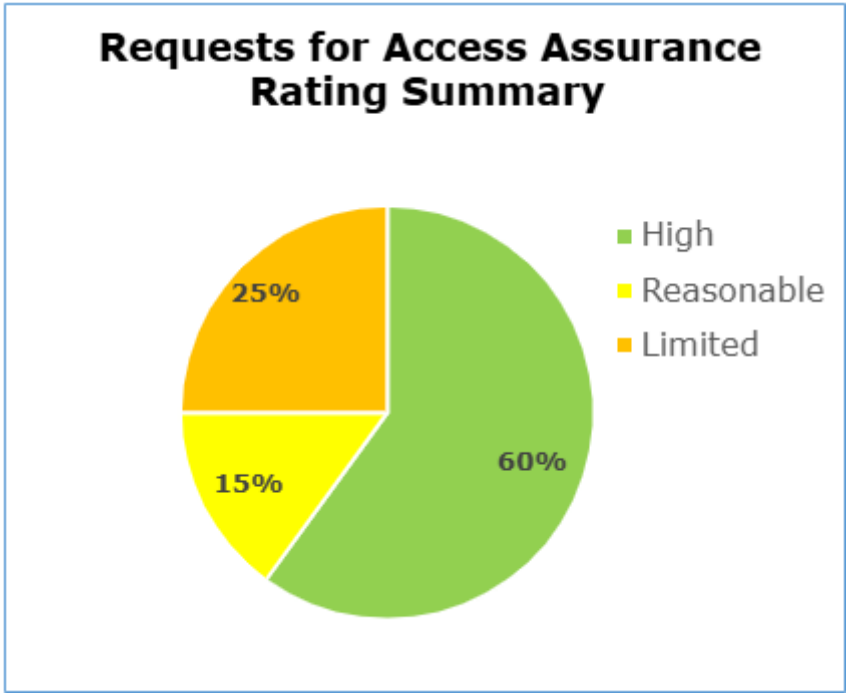
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Information and Cyber Security scope. 64% high assurance, 24% reasonable assurance, 12% limited assurance, 0% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 81% high assurance, 10% reasonable assurance, 6% limited assurance, 3% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 60% high assurance, 15% reasonable assurance, 25% limited assurance, 0% very limited assurance.

Key areas for improvement

We identified some key areas within our audit, where the Trust needed to implement further measures to comply with data protection and FOI legislation.

Information and Cyber Security

- While the Trust have an overarching classification policy in use for broad categories of information, it is not consistently applied to all documents containing personal information.
- The Trust are not currently deleting, destroying or archiving any personal information due to the Infected Blood Enquiry. The Trust could be retaining personal data that is not relevant to the enquiry beyond its retention period.
- Removeable media issued by the Trust is not logged on any asset register and therefore is not being flagged for collection upon leaving the Trust.
- The Trust routinely assess access rights for high-risk areas, however similar checks are not done for all staff areas. There is a contingency plan in place to remove access for any cards not in use after a six week period, however this risks that unauthorised personnel have retained access to hospital sites.
- The Trust has found that some of the accounts on their systems have level of access inappropriate to their role. We do note that the Trust has a plan to limit the amount of privileged/administrator accounts, removing access rights for staff that no longer require privilege/ admin accounts.
- Review of access rights is not done consistently across the Trust, and there has been instances where users access rights have not been changed promptly.
- The Trust has some legacy systems in place. Although these have been risk assessed and approved by appropriate senior management, systems which are outside of their support lifespan are vulnerable to cyberattack.

Freedom of Information

- The Trust does not currently have a mechanism which would ensure that staff are informed of any changes to policies and procedures regarding FOI/EIR regulations.
- The Trust does not have a written procedure in place which outlines how to deal accurately with hybrid requests which merge FOI/EIR requests with a subject access request (SAR).
- The Trust does not have a written procedure outlining how to identify and respond to vexatious requests (sS.14(1) FOIA) and manifestly unreasonable requests (reg 12(4)(b) EIR) in line with the legislation.

Requests for Access

- The interviews have shown that some staff do not know how to recognise and deal with verbal SARs nor how to document them.
- There is no easily accessible guidance for staff which outlines how to recognise and respond to a SAR and where to channel a SAR.
- The Trust does not inform the requester about their right to lodge a complaint with the ICO, as suggested by the SAR response template.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

Information and Cyber Security

- It was evidenced during the audit that there are key lines of communication, not only between the teams but also in the reporting lines of data protection matters. This included both up to the Board but also across multiple hospital sites for consistency. The Cyber Security team and management also demonstrated that they are active within the cyber security community and are actively horizon scanning for potential best practices and risks.
- There is a clear process for integration of information and cyber security related changes into project management to ensure the risks are addressed throughout the project lifecycle. Requests for change must be approved by the Change Advisory Board (CAB). Furthermore, risk management is documented in appropriately detailed data protection impact assessments (DPIAs).
- DPIAs are completed before engaging new suppliers to understand and mitigate risks prior to IT suppliers being granted access to the organisation's networks and / or assets.

Freedom of Information

- There is clear governance oversight in place to ensure compliance with FOI regulations. FOI figures are regularly collated and presented at Information Governance Group (IGG) meetings.
- Staff outside of the FOI team received FOI specialist training to build team resilience.
- The Trust proactively publishes all FOI disclosures on their external website.
- The FOI team builds and maintains positive working relationships with teams which provide information for FOI disclosures. The interviewed staff from across the Trust showed good knowledge of internal FOI

procedures and fulfilled their FOI related responsibilities to a good standard. Altogether, the FOI team has good visibility across the Trust.

- The Trust has robust logs where FOI handling is recorded including the FOI Database, which informs the reports presented at IGG. The information is detailed and ensures for informative reports.
- The Trust has a system of frequent and periodic dip sampling of FOI requests, which is followed by feedback to staff. This includes a review of redactions.
- The FOI team is active in FOI networks, which allows it to keep up to date with FOI news and developments.

Requests for Access

- There are clear governance structures to provide appropriate oversight of SAR processes and performance. They ensure appropriate escalation of SAR matters and figures.
- The Trust has robustly documented procedural documentations for various aspects of SAR handling, like information collation or redactions.
- The SAR Database used to manage SARs requires to log a high amount of information about the requests, which ensures that SAR handling records are detailed and robust.
- The SAR Database and the Nalytics redactions software automatically log information on all actions like the name of the person who performed the action, date and time. This allows for a clear and robust audit trail.
- The Trust uses FileShare to disclose information, which provides a link to the requested documents and a password in a separate email. Furthermore, it informs the Trust when the information was downloaded and by whom.
- The Trust has a system of frequent and periodic dip sampling of SAR requests, which is followed by feedback to staff.

Best Practice

Information and Cyber Security

- The Trust have a robust risk management framework in place which demonstrates that any new, high or change in risks is regularly discussed at various groups and committees. There is a method for highlighting not only direct risks but also any risks with a IG/CS element. There is also an embedded review process which ensures that high risks are reviewed regularly for oversight.

Freedom of Information

- The Trust has put considerable effort into creating an engaging training programme using the Vyond software, with considerable input from the FOI and SAR teams. The training is a combination of videos which are created by the Trust and bespoke to its needs and quizzes to test staff knowledge.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Liverpool University Hospitals NHS Foundation Trust.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Liverpool University Hospitals NHS Foundation Trust. The scope areas and controls covered by the audit have been tailored to Liverpool University Hospitals NHS Foundation Trust and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.