Royal Free London NHS Foundation Trust

Data protection audit report

January 2024

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) 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.

Royal Free London NHS Foundation Trust (the Trust) agreed to a consensual audit of its data protection practices.

The purpose of the audit is to provide the Information Commissioner and 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 legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust’s processing of personal data. The scope may take into account any data protection issues or risks which are specific to the Trust, identified from ICO intelligence or the Trust’s own concerns, or any data protection 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
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.
Ad Hoc Disclosures	The extent to which the organisation has in place measures to manage 3rd party ad hoc requests for personal data and to prevent inappropriate disclosures

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 and a series of interviews with key staff members.

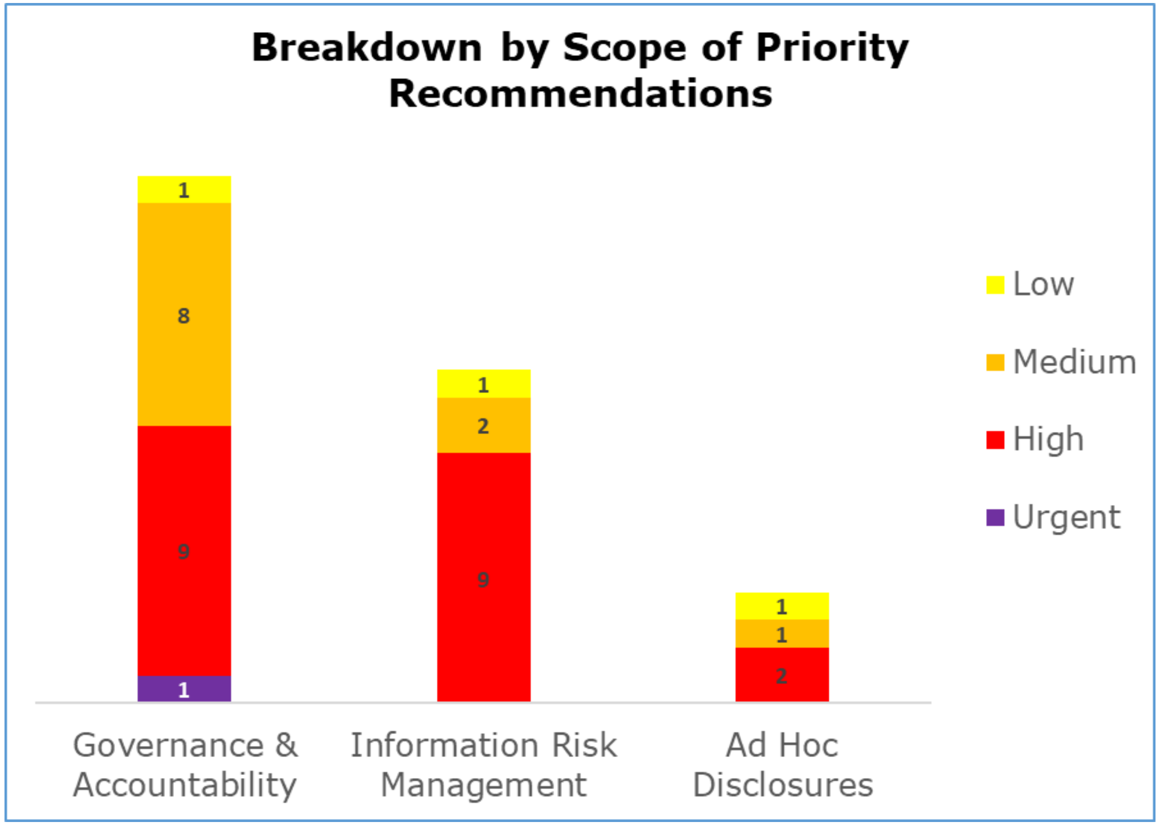
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that 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
Governance and Accountability	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.
Information Risk Management	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.
Ad Hoc Disclosures	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.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

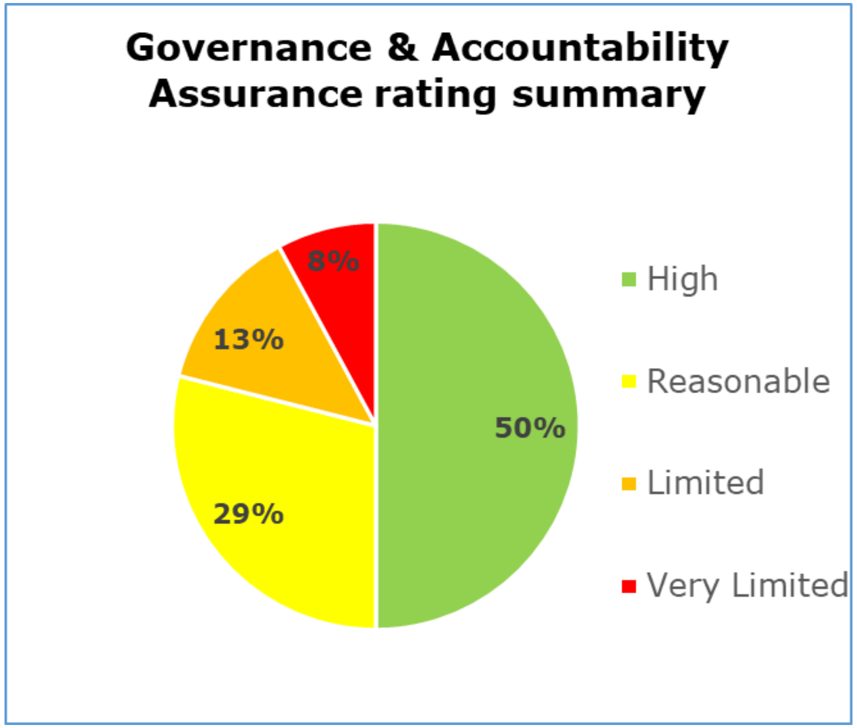


The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

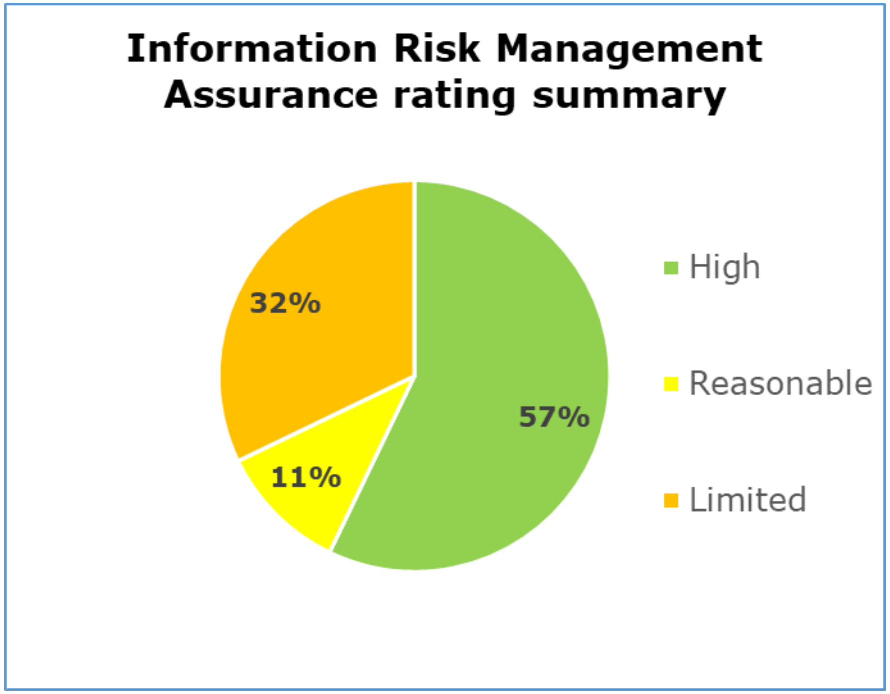
- The Governance and Accountability scope has 1 urgent, 9 high, 8 medium and 1 low priority recommendations.

- The Information Risk Management Scope has 0 urgent, 9 high, 2 medium and 1 low priority recommendations.
- The Ad Hoc Disclosures scope has 0 urgent, 2 high, 1 medium and 1 low priority recommendations.

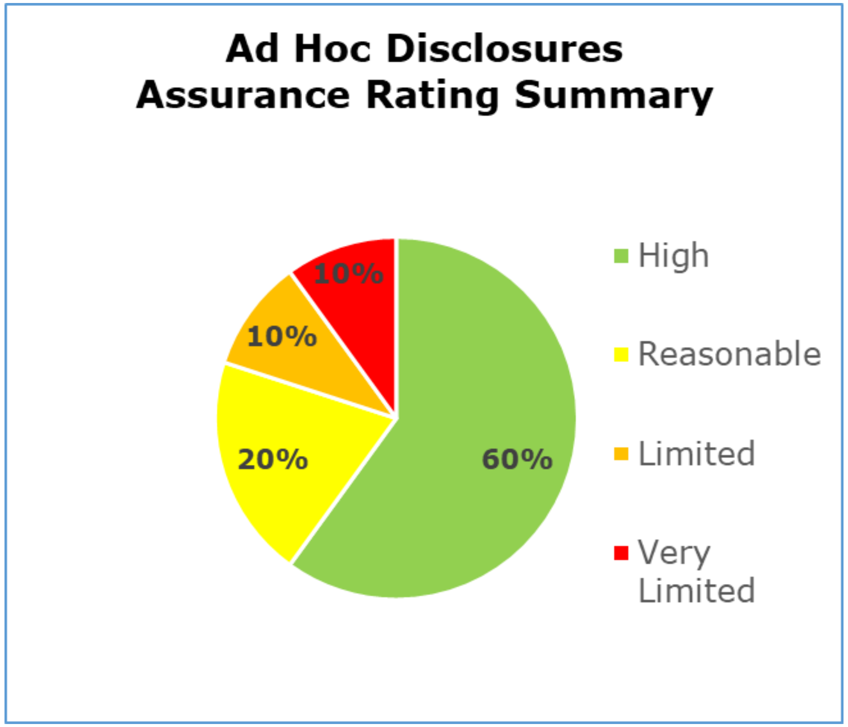
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 50% high assurance, 29% reasonable assurance, 13% limited assurance, 8% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 57% high assurance, 11% reasonable assurance, 32% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Ad Hoc Disclosures scope. 60% high assurance, 20% reasonable assurance, 10% limited assurance, 10% very limited assurance.

Areas for Improvement

Governance and Accountability

- A formal, comprehensive and documented Record of Processing Activities (ROPA) must be completed in order to ensure that the Trust meets its responsibilities under data protection legislation.

- Periodic compliance checks are not undertaken on all the Trust's data processors. Without this, the Trust cannot have assurance that the processors are complying with their contracts and with data protection legislation.

- Mandatory information governance training compliance is not at a high enough level, with the risk that personal data breaches may be caused by a lack of knowledge among staff.

- There needs to be an effective process in place to ensure that paper records are managed in accordance with the Trust's retention schedule so that records are not kept beyond the time required by regulations.

Information Risk Management

- The Trust is currently lacking a robust process to ensure that all Data Protection Impact Assessments (DPIAs) are reviewed on a periodic basis, or when there is a change to the nature of the scope or purposes of the project, which means that new risks which could occur may not be adequately mitigated, and could lead to data breaches.

- A system of Information Asset Owners (IAOs) has not been fully rolled out across the Trust, and some IAOs have not had specialist risk management training to enable them to fulfil those roles effectively.

Ad Hoc Disclosures

- At present, the Trust does not record an appropriate UK GDPR lawful basis prior to the disclosure of personal data in response to an ad hoc request for personal data, leading to a risk of unlawful or inappropriate disclosures being made.

- The Trust needs to make some improvement in relation to the processing of personal data in CCTV and Body Worn Video images and footage. A documented procedure should be in place concerning the identification and implications around third party data in these cases. There should also be appropriate technical means in place to redact the footage and still images, backed up with training and guidance for staff.

Best Practice

Governance and Accountability

- The Trust's main privacy notice on its web page has an embedded video which explains in plain language with visual aids, how the trust uses personal data, which is a clear and effective way to convey privacy information.

- The Trust conducts confidentiality audits. These audits cover all three main hospital sites and largely focus on staff awareness at each locality of IG matters such as the requirement to undertake annual mandatory IG training or how to report an IG incident. Annual results and key findings of the confidentiality audits are reported to the Information Governance Group (IGG) for information.

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 Royal Free London 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 Royal Free London NHS Foundation Trust The scope areas and controls covered by the audit have been tailored to Royal Free London NHS Foundation Trust and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.