Moorfields Eye Hospital 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.

Moorfield Eye Hospital 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
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
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.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

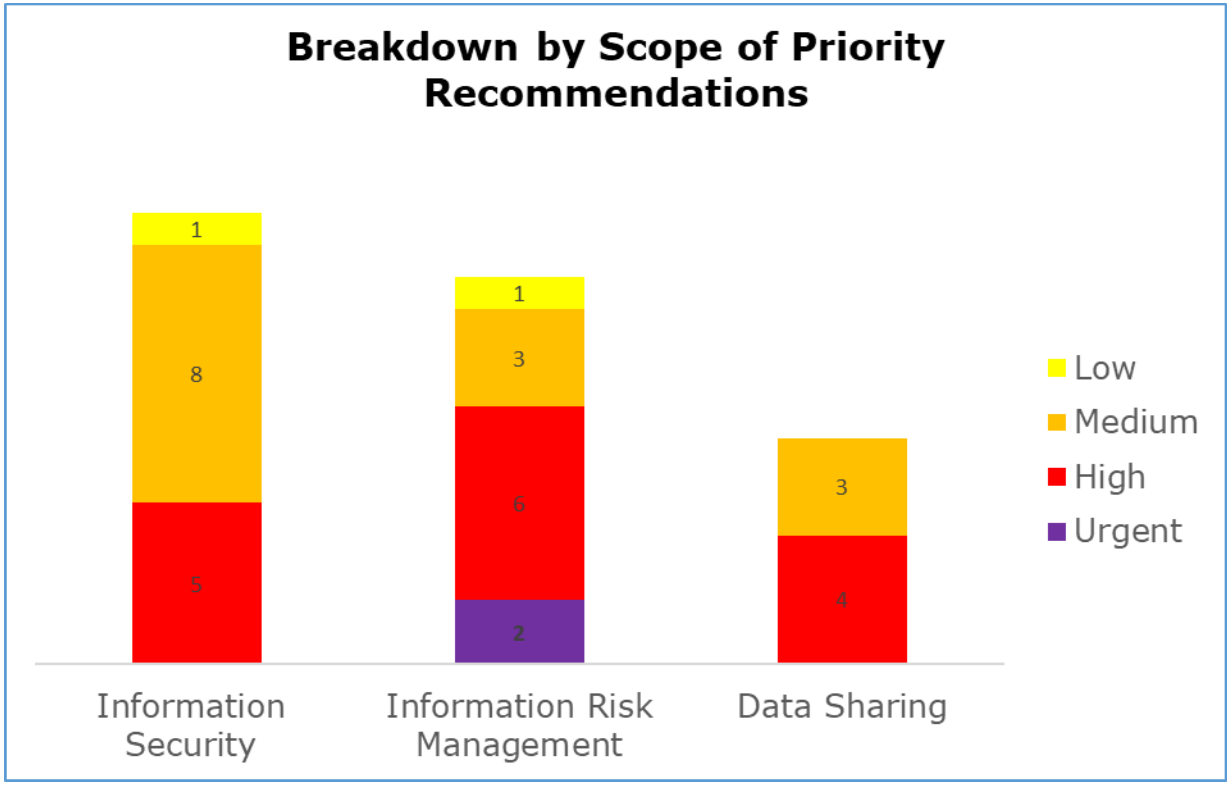
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential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

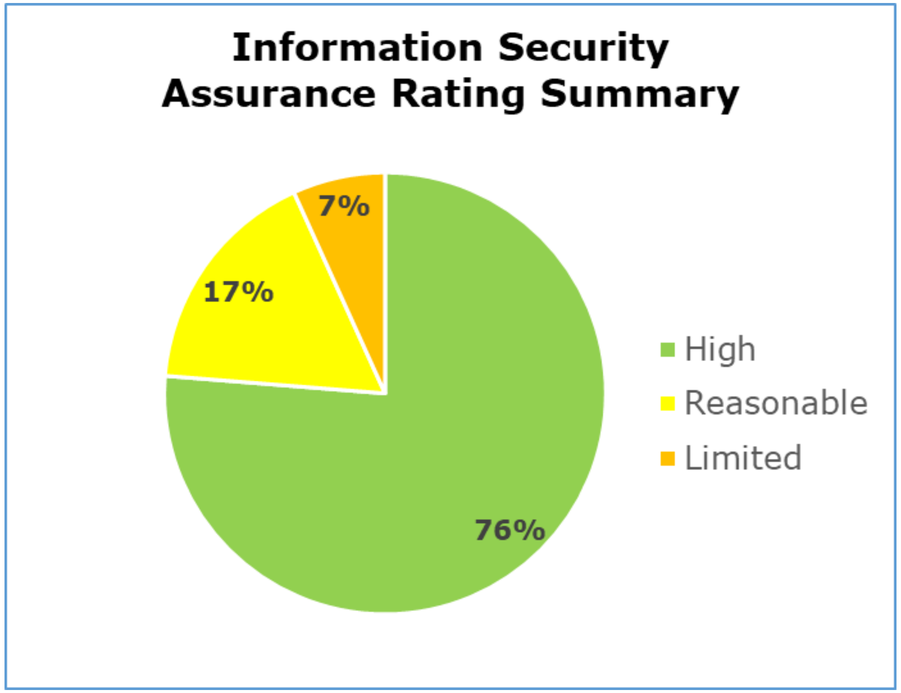
Priority Recommendations



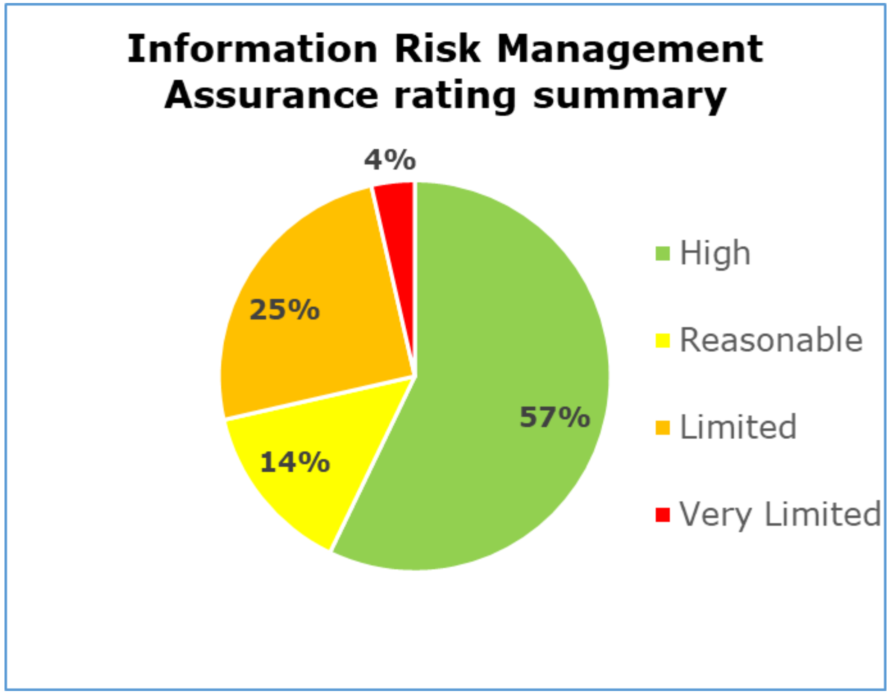
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Information Security has 0 urgent, 5 high, 8 medium and 1 low priority recommendations
- Information Risk Management has 2 urgent, 6 high, 3 medium and 1 low priority recommendations
- Data Sharing has 0 urgent, 4 high, 3 medium and 0 low priority recommendations

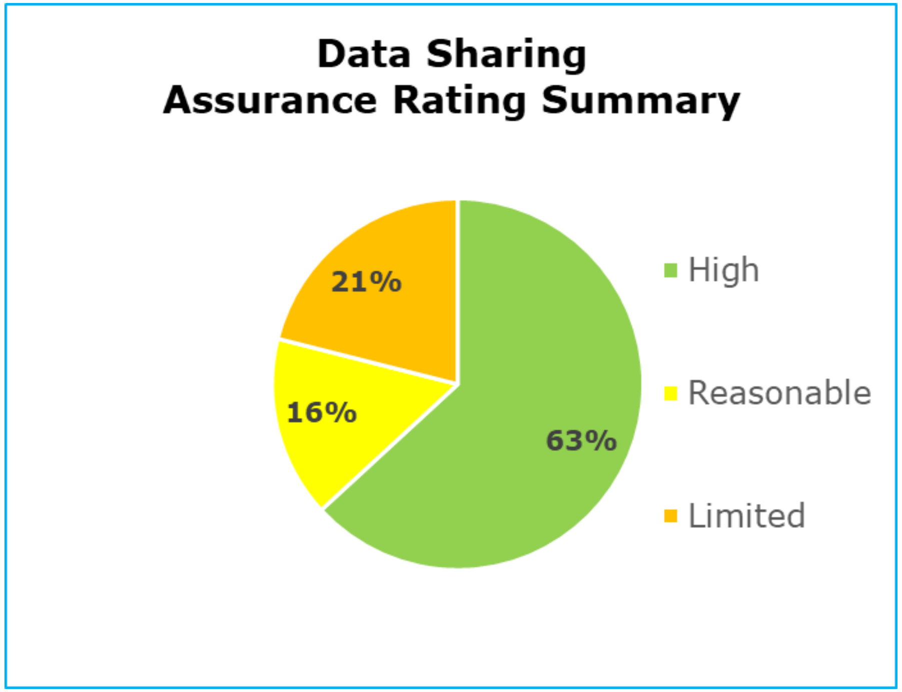
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Information Security Scope: 76% high assurance, 17% reasonable assurance, 7% limited assurance, 0% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 57% high assurance, 14% reasonable assurance, 25% limited assurance, 4% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 63% high assurance, 16% reasonable assurance, 21% limited assurance, 0% very limited assurance.

Areas for Improvement

Information Security

- The permanent roles which make up the Information Security function should be filled quickly to ensure that operational responsibility is clearly in place and embedded within the Trust
- The Trust should ensure that a template letter is in place to notify data subjects of a data breach which includes all appropriate information including details of the DPO, a description of the likely consequences of the breach and the measures which have been taken about the breach.

Information Risk Management

- The Trust's DPIA process should include a record of the mitigations which have been put in place for identified risks, to provide assurance that these mitigations have been implemented
- DPIAs are not all currently kept under a regular process of review, leading to the danger of new risks which could emerge once the project is underway not being identified and therefore not being mitigated
- There is currently an information asset management improvement project underway at the Trust, once this is completed, the Trust must ensure that there are ongoing documented risk asse.sments of all the information assets which it holds to ensure that all risks are effectively controlled.

Data Sharing

- Appropriate reviewing processes should be in place for all Data Sharing Agreements, which include review schedules and review logs, in order to ensure that all data sharing is strictly controlled in line with the Data Sharing Code of Practice.
- The Trust should have measures in place to ensure that all staff likely to make decisions regarding data sharing receive appropriate training which is periodically refreshed.

Best Practice

- The Trust test their physical security on site, by means of police officers being shown round and then returning at a later date in plain clothes to assess the security, for example by seeing if they can get into secure areas or move around unchallenged without appropriate ID.

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