Imperial College Healthcare NHS Trust

Data protection audit report

September 2022

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 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 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.

Imperial College Healthcare NHS Trust (the Trust) agreed to a consensual audit of their 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, and/or any data protection issues or risks which affect their 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 & 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.
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.

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

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, the Trust agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews was conducted from 19 to 22 July 2022. The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

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.

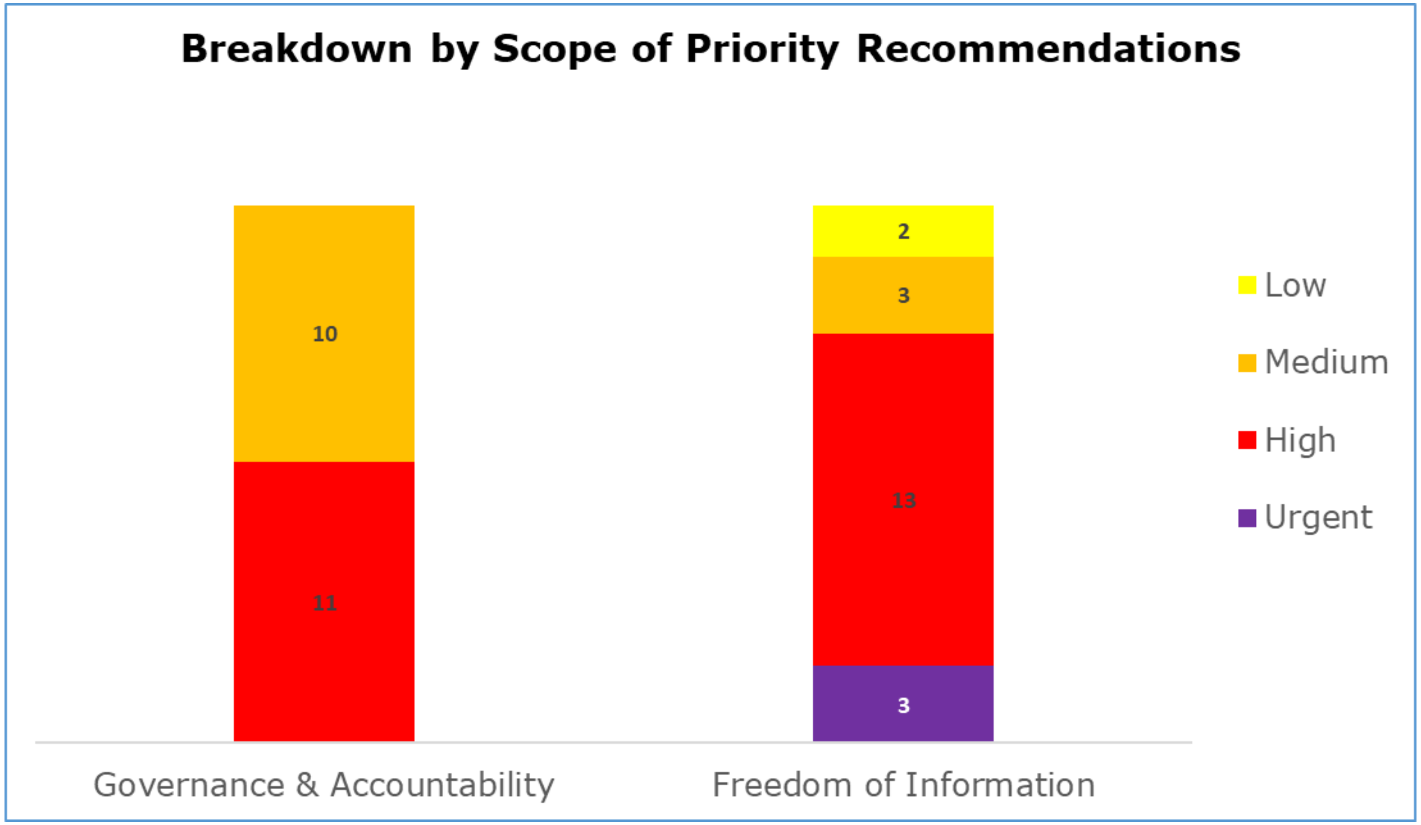
The ratings are assigned based upon the ICO's assessment of the risks involved. The Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance & 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.
Freedom of Information	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.

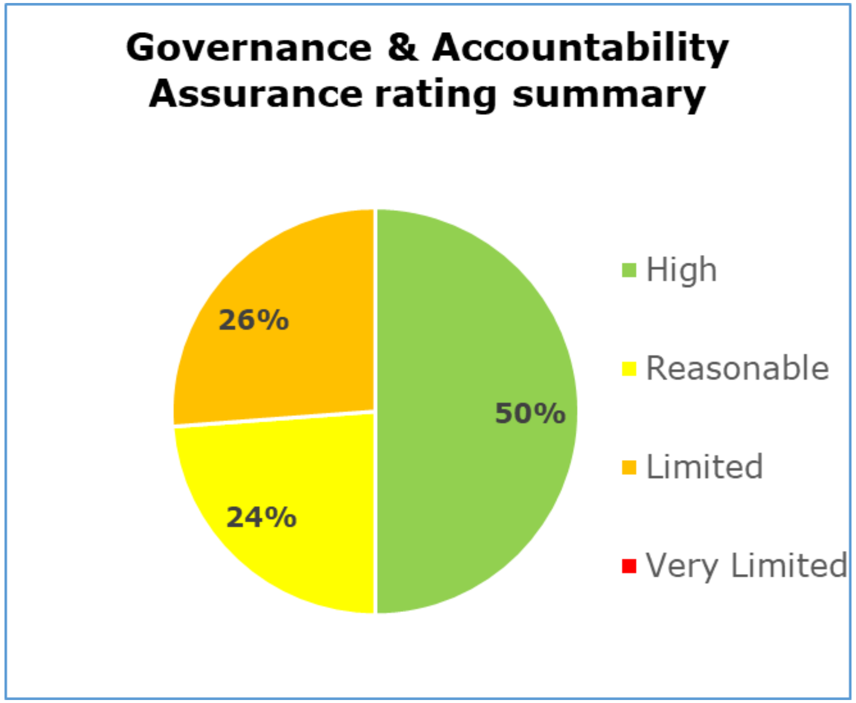
Priority Recommendations



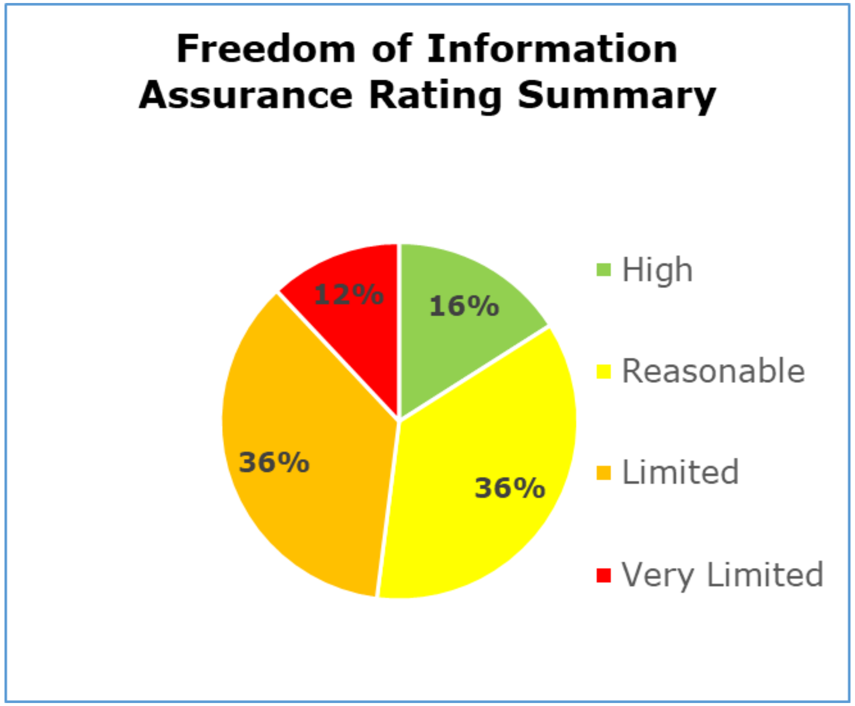
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has 11 high & ten medium priority recommendations
- Freedom of Information has three urgent, 13 high, three medium and two low priority recommendations

Graphs and Charts

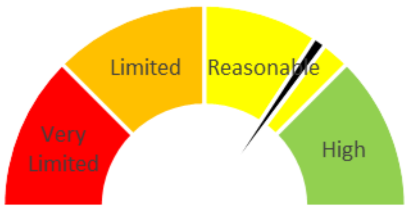


The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 50% high assurance, 24% reasonable assurance and 26% limited assurance.

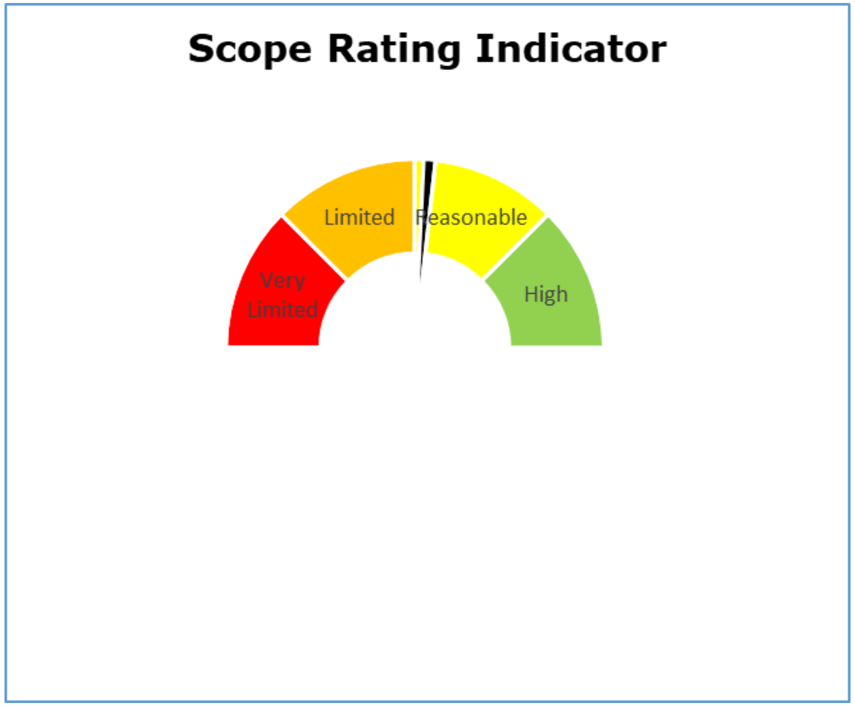


The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 16% high assurance, 36% reasonable assurance, 36% limited assurance, 12% very limited assurance.

Scope Rating Indicator



The speedometer chart above gives a gauge of where the organisation sits on our assurance rating scale from high assurance to very limited assurance for the Governance & Accountability scope area.



The speedometer chart above gives a gauge of where the organisation sits on our assurance rating scale from high assurance to very limited assurance for the Freedom of Information scope area.

Areas for Improvement

Governance & Accountability

- The Trust’s Induction process should include seeking assurances that key data protection policies have been read and understood by staff, to ensure they are aware of their data protection responsibilities.
- The Trust should ensure that the training needs for all staff with specialised data protection roles and functions across the Trust, such as the Caldicott Guardian and Information Asset Owners are identified and that the training is delivered and refreshed at an appropriate frequency.
- The Trust should complete any outstanding records of processing assessments as highlighted in the Records of Processing Report to ensure they hold a complete record of processing activities undertaken by the Trust.
- The Trust should ensure that routine compliance checks and audits are undertaken on its data processors after contracts have been signed, to provide assurance that the contract remains fit for purpose and that processors are complying with the terms and conditions.
- The Trust should work towards ensuring that all digital archived records are being deleted or destroyed in line with the Trust's retention policy.
- The Trust should ensure their Data Protection Impact Assessment (DPIA) procedure is embedded within all the main procurement, project and change management policies and procedures. The policies should stipulate the requirement to undertake DPIA screening and completion where necessary.

Freedom of Information

- The Trust should ensure that it has policies and procedures in place which document its approach to complying with the Environmental Information Regulations (the EIR) including responsibility for responding to requests and overseeing performance.
- Induction training for new staff requires review to ensure it includes recognising and dealing with FOI or EIR requests. Regular refresher training on the EIR should also be included within the mandatory training for all staff.
- The Trust's publication scheme should be reviewed so that all the information which is in the public interest and safe to disclose is available and to ensure that environmental information is proactively published as required. The Trust should also ensure that information about how to make an EIR request is publicly available.
- The Trust should examine the resources provided for the handling of FOI and EIR requests so that responses can be dealt with within statutory timescales, and the FOI Manager is also able to deal with their other responsibilities.

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