

University Hospitals Plymouth NHS Trust

Data protection audit report

September 2021

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 sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The audit was undertaken consensually and as part of our annual audit programme.

The purpose of the audit is to provide the Information Commissioner and University Hospitals Plymouth NHS 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 legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust 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 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 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 UKGDPR and national data protection legislation are in place and in operation throughout 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 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 were conducted from 2 August 2021 to 13 August 2021. 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 priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

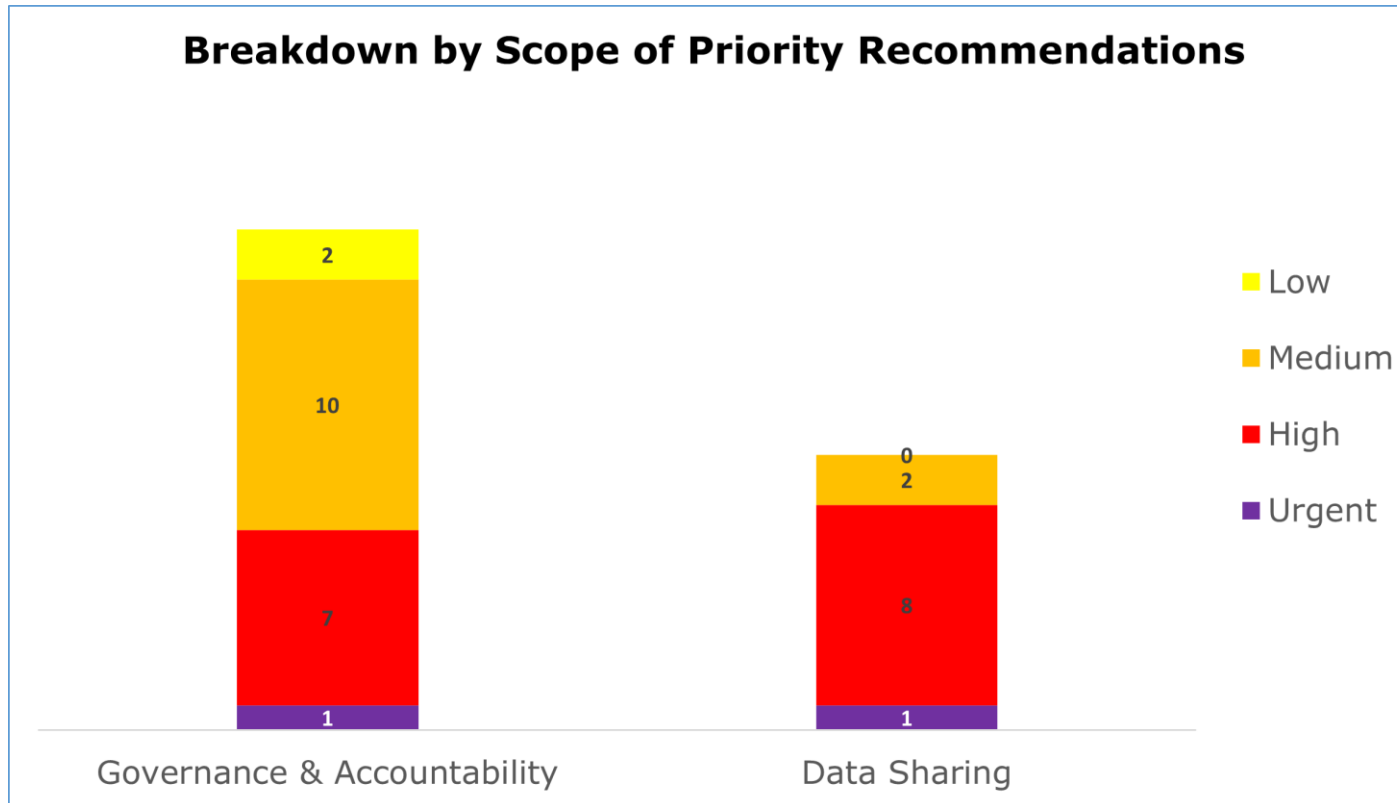
Audit Summary

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.
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.

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

Priority Recommendations

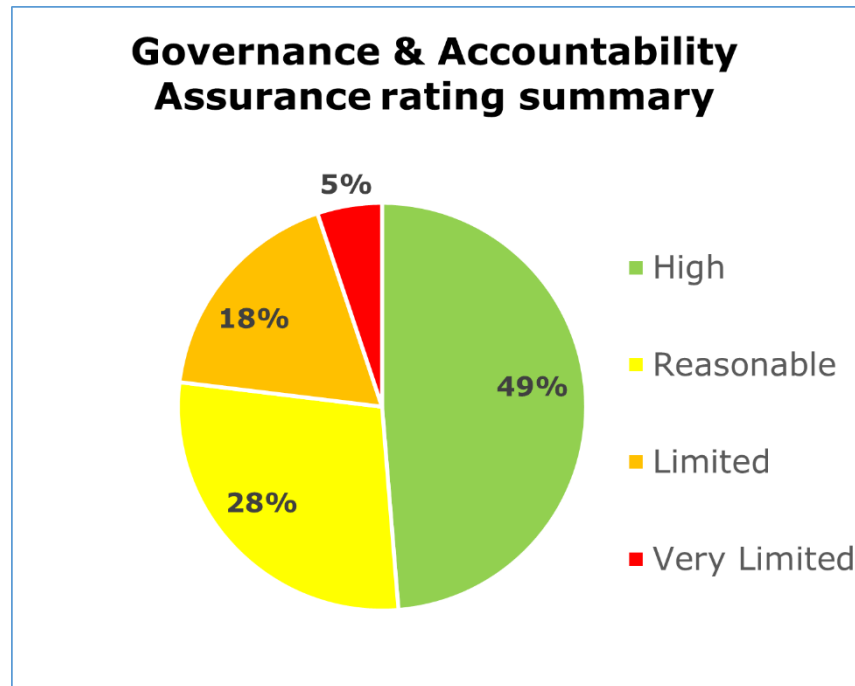
A bar chart showing a breakdown by scope area of the priorities assigned to the recommendations made.



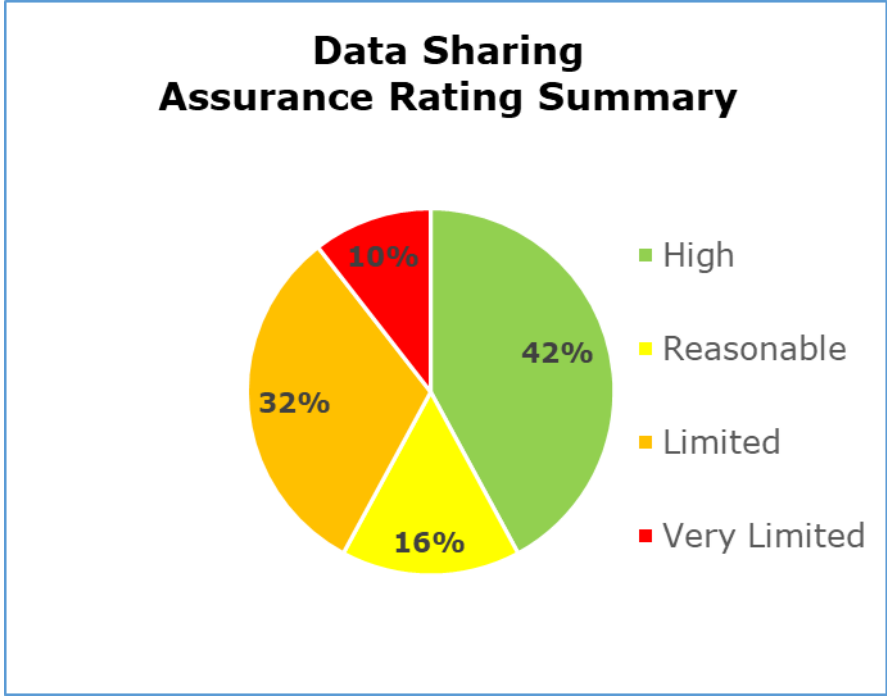
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has 1 urgent, 7 high, 10 medium and 2 low priority recommendations
- Data Sharing has 1 urgent, 8 high, 2 medium and 0 low priority recommendations

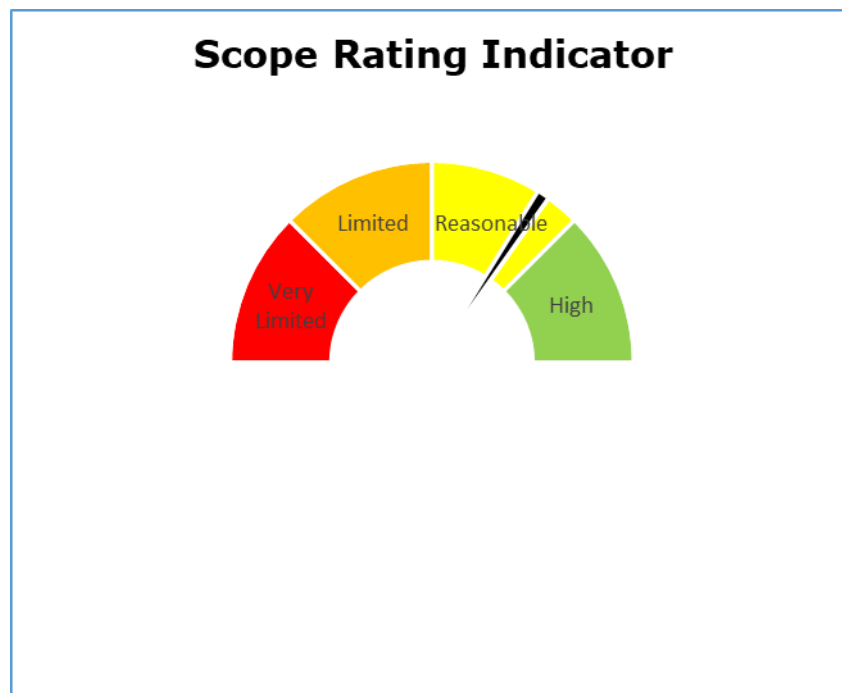
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 49% high assurance, 28% reasonable assurance, 18% limited assurance, 5% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 42% high assurance, 16% reasonable assurance, 32% limited assurance, 10% very limited assurance.



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

Areas for Improvement

Governance & Accountability:

- It was identified that the Trust does not have an Appropriate Policy Document (APD) in place. The Trust should ensure they have an APD in place or make sure that it has documented its decision where it is determined an APD is not required and the reasons for this decision.
- The Trust's DPIA process requires improvement. Currently, a full DPIA is required to be completed for every new or change to a project or system. However having an effective screening process at an early stage of the project will ensure that a DPIA is only undertaken when the processing of personal data is likely to result in a high risk to individuals' rights and freedoms and early enough in the project to provide assurances that the appropriate data protection considerations have been assessed and measures to mitigate any risks put in place.
- Some specialist data protection roles have not undertaken role specific refresher training post GDPR.

Data Sharing:

- Further to the point made above, data sharing training has also not been provided to staff who are involved in this process, and this training requirement has not been identified as part of the Trust's Training Needs Analysis (TNA) review.
- There is no central log or other mechanism in place which would enable the Information Governance (IG) Team to maintain a level of oversight of all Data Sharing Agreements (DSA) across the Trust.
- Retention and disposal arrangements for personal data have not been agreed with all sharing partners within DSAs.

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.