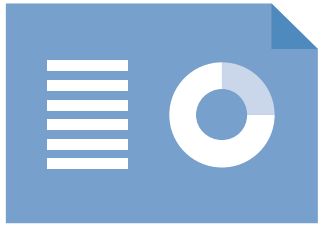
Nottingham University Hospitals NHS Trust

Data protection audit report

November 2020

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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 purpose of the audit is to provide the Information Commissioner and Nottingham University Hospitals 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.

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 GDPR 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 28 September to 8 October 2020. 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

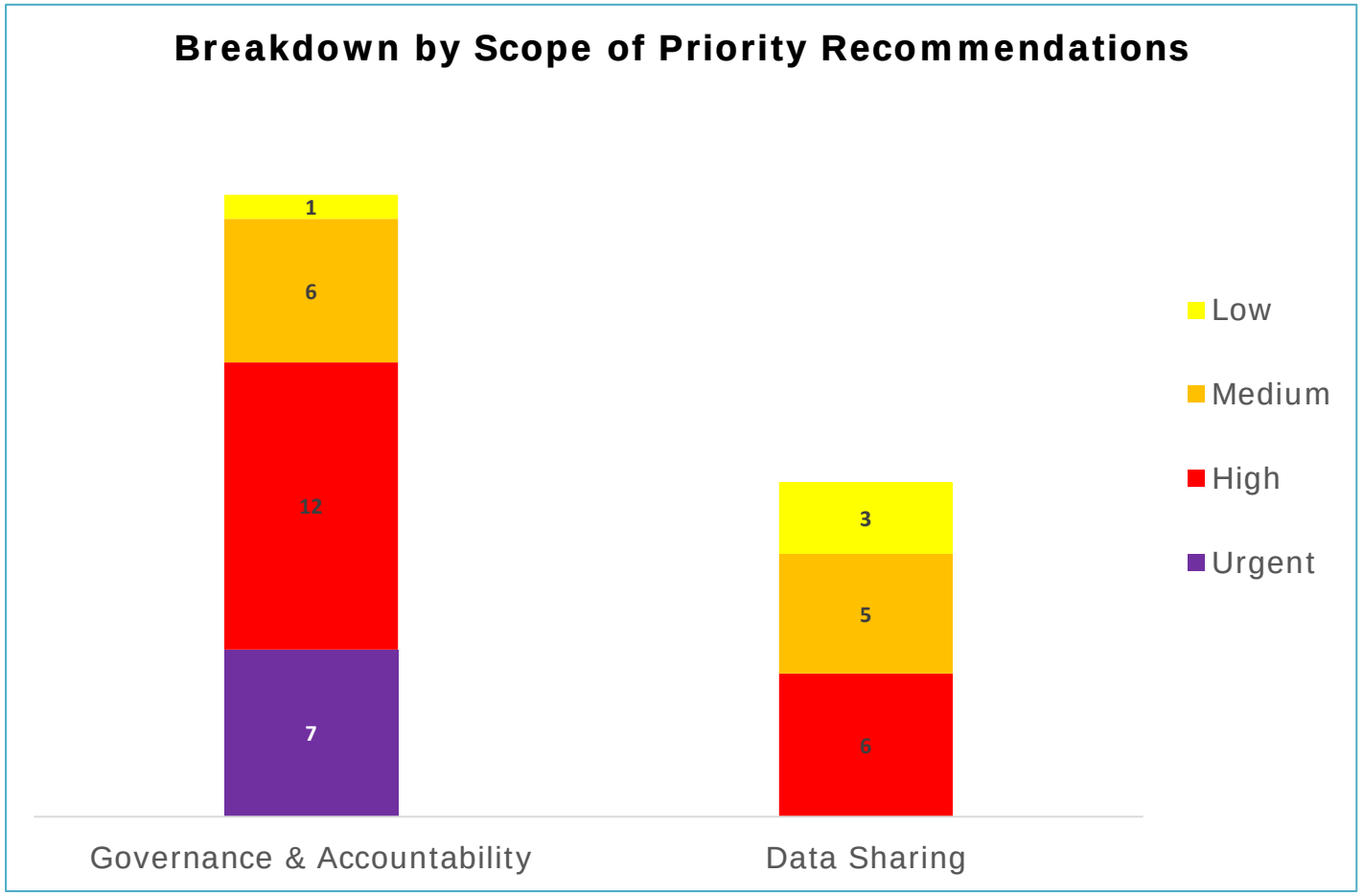
recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary*

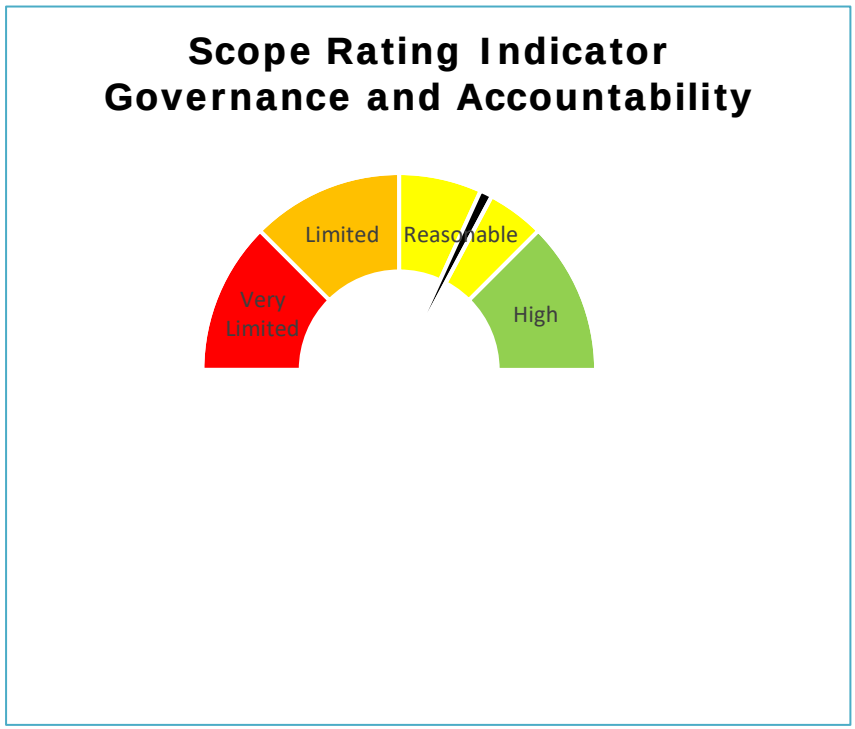
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
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.

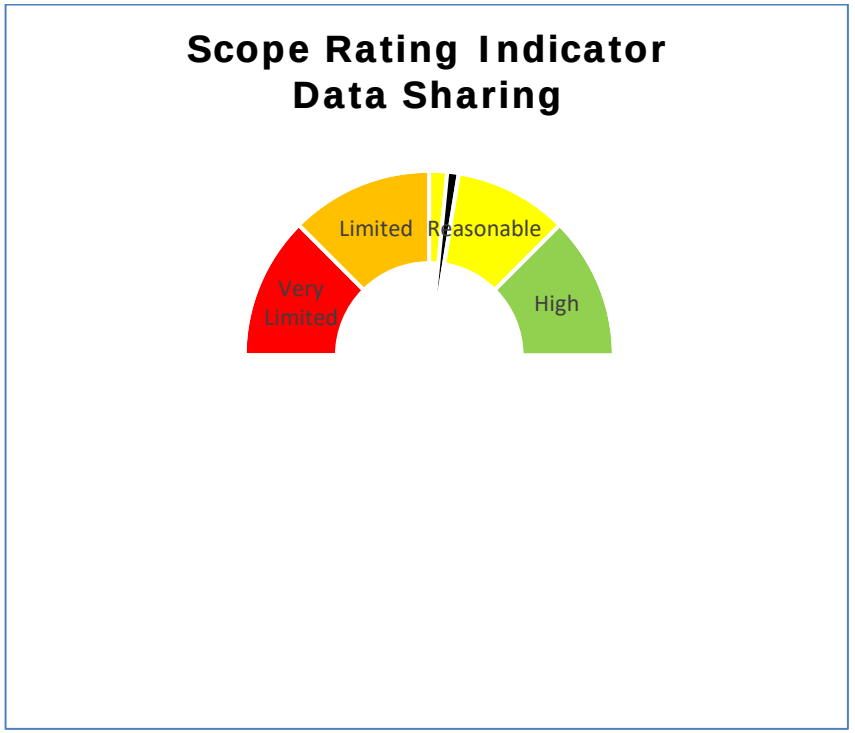
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations



Graphs and Charts





Areas for Improvement

Governance and Accountability

- The Trust needs to determine whether they require an Appropriate Policy Document in place which documents their justification for processing personal data to ensure that they are not in breach of Schedule 1 of the DPA 2018.

- The Trust needs to put in place a full Record of Processing Activities in order to ensure they have full and detailed knowledge of all data processing taking place across the Trust.

- Mandatory refresher data protection training must be completed by all staff, otherwise there is a risk of staff not having adequate knowledge to avoid data protection breaches.

- The Trust should continue with its work to account for, log and review all data processing agreements in a timely manner to reduce the risks of non-compliance with the appropriate legislation.

Data Sharing

- Not all data sharing agreements (DSAs) contain sufficient detail and procedures to provide adequate direction to each party and thereby ensure that the requirements of the legislation are met.

- The Trust needs to put in place a formal review process for existing data sharing agreements to mitigate risks of unlawful sharing.

- Ongoing evidence should be obtained by the Trust to provide assurance that the access controls agreed with sharing partners are being implemented as arranged.

- The Trust should ensure that there is in place a consistent process to evidence that the deletion of shared data is being undertaken by third parties in data sharing in line with contractual agreements.

Best Practice

The Trust makes exemplar copies of good practice in completing DPIAs available on the Information Governance pages of the Trust Intranet.

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 Nottingham University Hospitals NHS Trust (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.