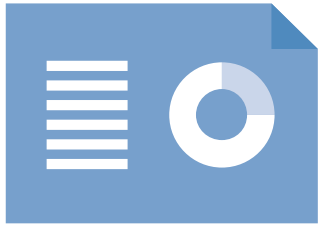
Camden and Islington NHS Foundation Trust

Data protection audit report – Executive Summary

July 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.

Camden and Islington NHS Foundation Trust (the Trust) agreed to a consensual audit in October 2019. Two audit scopes were agreed. However, due to the organisational pressures created at the Trust by Covid – 19, it was agreed that the remainder of the engagement would be postponed until later this year. Two separate reports will be produced, of which this is the first.

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.

It was agreed that the first part of the engagement would focus on the following area:

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 GDPR and national data protection legislation 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.

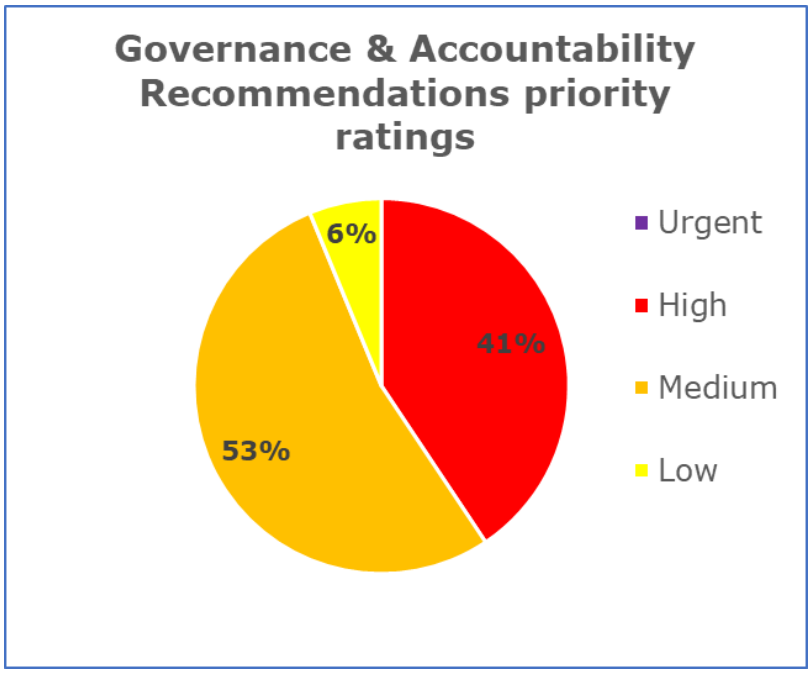
However, due to the outbreak of Covid - 19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, the Trust agreed to continue with the audit on a remote basis. As the Trust responded to mounting Covid – 19 pressures, auditors worked with representatives of the Trust to adapt a flexible work around to complete the audit. A desk-based review of selected policies and procedures and remote telephone interviews were conducted from 11 – 22 May 2020. The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

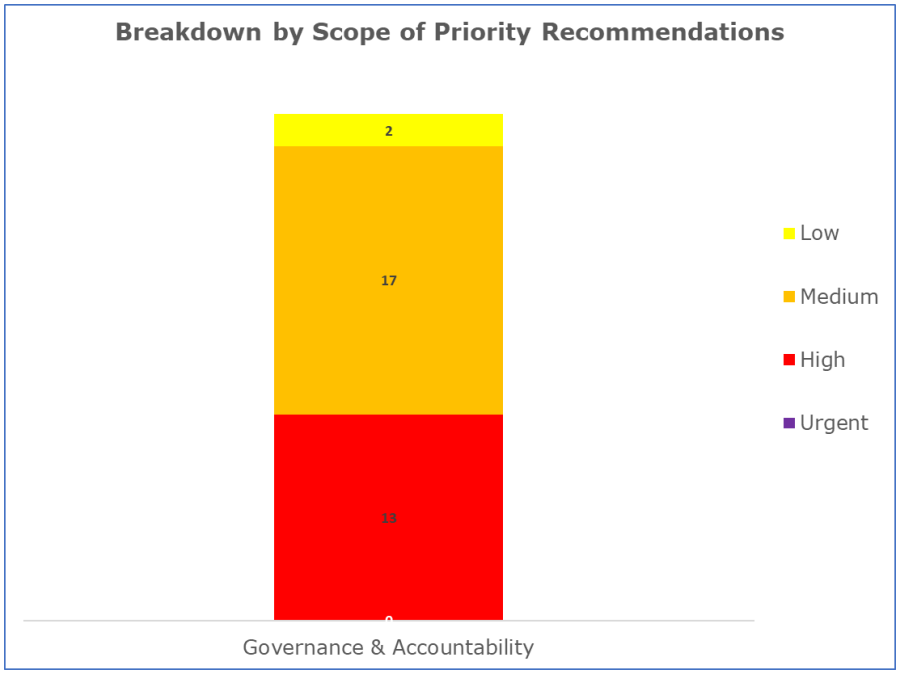
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Camden and Islington NHS Foundation Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

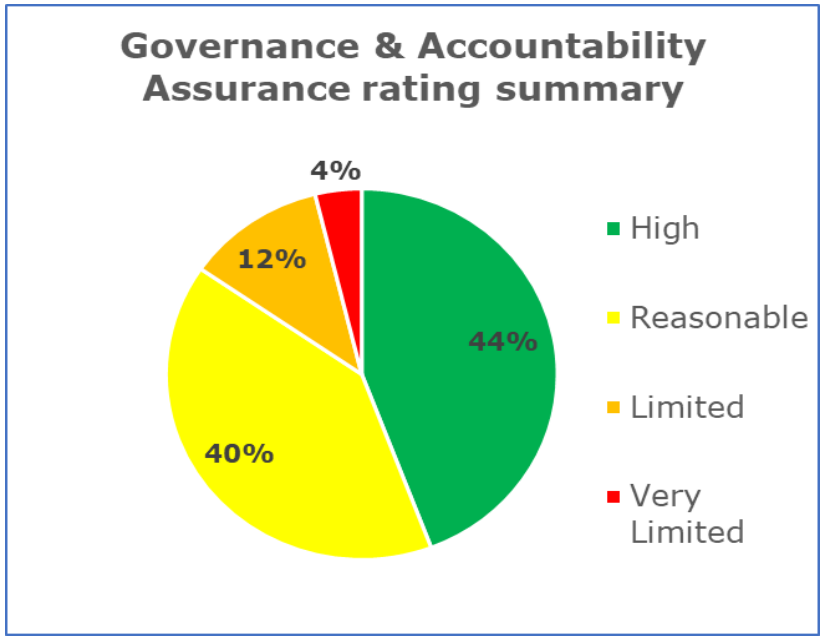
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce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

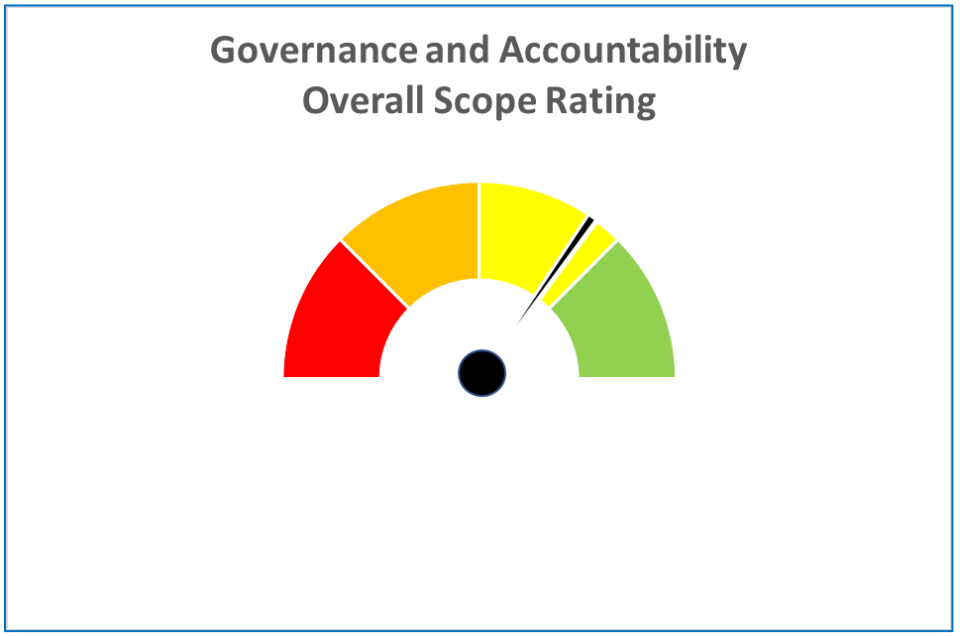
Priority Recommendations





Graphs and Charts





Areas for Improvement

The Trust should review its resilience and task allocation around the wider Information Governance (IG) team to ensure continued functioning.

Robust, proactive monitoring mechanisms are needed to ensure compliance with data protection policies.

All staff, including agency staff, should receive appropriate IG training prior to being granted access to personal data.

When rolling out the Information Asset Management tool, Flowz, the Trust needs to ensure that it is accurately capturing all data processing. It promises to be a useful tool if it also encompasses all relevant information pertaining to processing such as DPIA's, processor contracts etc, but will only be effective if the processes of keeping it up to date are embedded in practice.

A clear process is required to notify individuals when there has been a data breach which is likely to result in a high risk to their rights and freedoms. There are currently no templates to provide appropriate information to individuals whose data has been breached.

Best Practice

The Trust provided Privacy Information in a timely manner when a national health emergency occurred and highlighted how personal information could be processed in such circumstances.

The IG Intranet page is a 'one-stop shop' for a comprehensive range of materials for staff including links to policies and guidance, links to the Information Asset Owner handbook and other Information Asset Management information, posters and a link to the front end of Datix if staff need to report an incident. There are also explanations of who the SIRO, Caldicott Guardian and DPO are with their contact details.

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