South London and Maudsley NHS Foundation Trust

Data protection audit report – Executive Summary

August 2021

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 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 South London and Maudsley NHS Foundation 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'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 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 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 13/07/2021 to 16/07/2021. The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

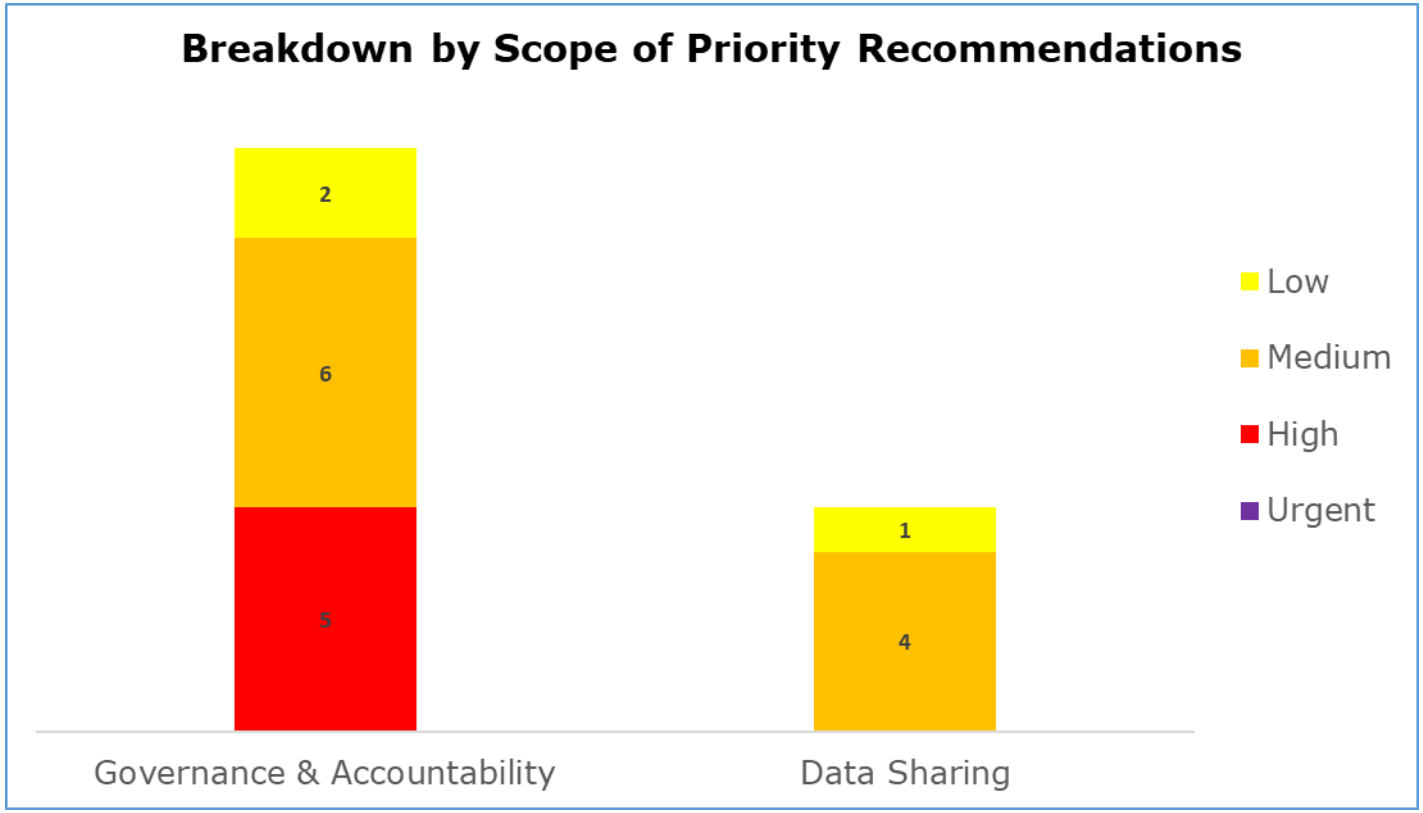
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that 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 and Accountability	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.
Data Sharing	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.

*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.

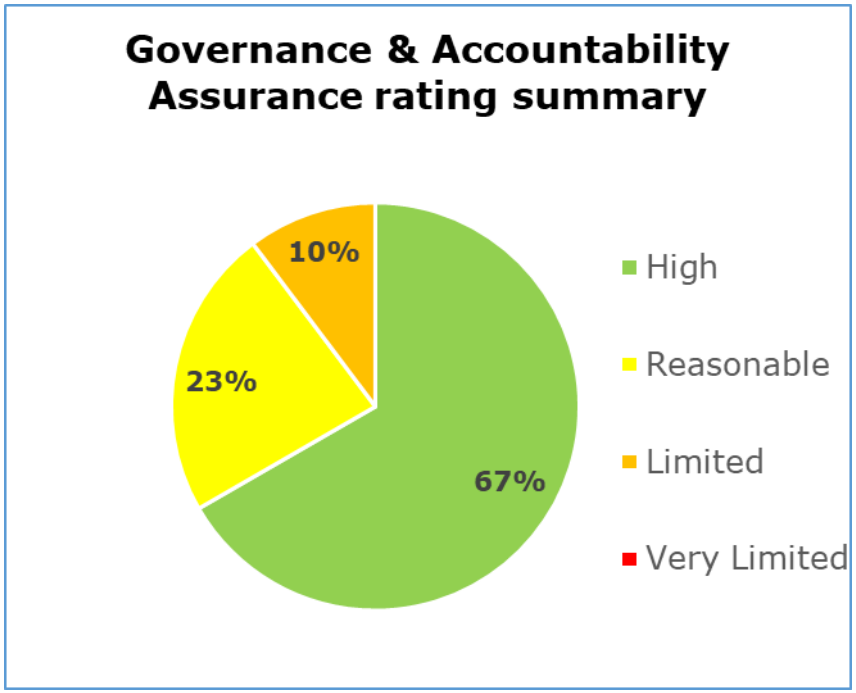
Priority Recommendations



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

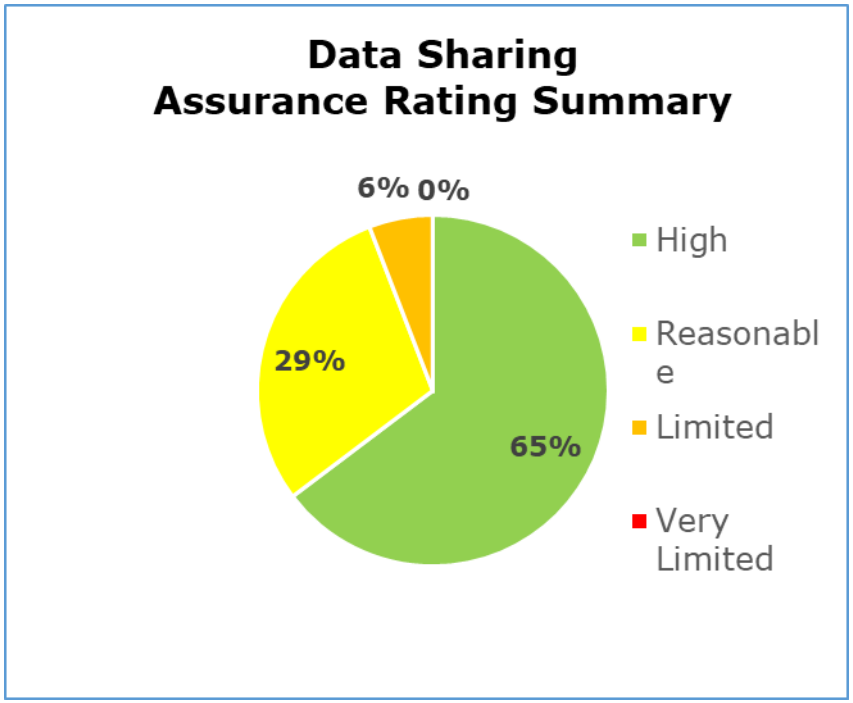
- Governance and Accountability has 5 high, 6 medium and 2 low priority recommendations
- Data Sharing has 1 high and 4 medium priority recommendations

Graphs and Charts



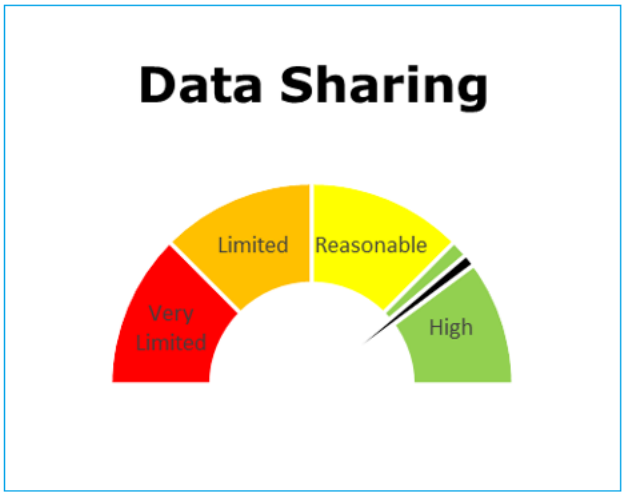
The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope.

- 67% high assurance
- 23% reasonable assurance
- 10% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 65% high assurance

- 29% reasonable assurance
- 6% limited assurance.



This 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

The Trust has not completed a comprehensive record of processing activities (RoPA), in line with the requirements set out in Article 30 of the UKGDPR.

While there are means for data protection information to be disseminated to staff via team meetings, and staff can make use of the Information Governance (IG) department's Yammer channel, there are no operational level IG focussed groups in distinct divisions or sections of the organisation. This may result in direction from senior management not being implemented or embedded on a local level, as well as 'on the ground' problems not being communicated or reported to senior management in a timely fashion. This is also reflected in the survey result which indicated that 23% of survey respondents would not know where to go for data protection advice.

Whilst the Trust's face to face IG training is highlighted below as best practice it is currently only available on request or at departmental level. This means that individuals in departments responsible for roles that carry higher information risks (such as SAR/disclosure admin, or information asset owners and administrators) may not be able to get enhanced training creating a greater risk of errors. The Trust has identified that those who share data require enhanced training, however they currently only provide this training on request or to departments who share data under sharing agreements, which risks missing the individuals in departments who are responsible for collating, redacting and sending information in response to ad hoc requests.

Best Practice

Once it is reinstated, the Caldicott Committee should become an effective means of collaboration and awareness within the Trust and should help provide assurance that the interests of data subjects are embedded in Trust-wide philosophies and practices.

The Trust produces a number of 'Policy on a Page' documents which provide a high-level summary (one page in length) of a policy to enable staff to remember key points.

Despite the effects of the Covid 19 Pandemic making normal site audits of data protection compliance difficult, the Trust has looked at other ways to provide assurance at this time, such as providing materials for self-assessment, and providing photographic evidence that the confidential waste process is taking place properly.

The Trust's board members undergo specialised IG training on an annual basis. This gives senior decision makers an enhanced understanding of the intricacies of information governance and compliance with legislation.

The IG team provide face to face training on request and to those groups they identify as benefitting most from it. The face to face training is based on the content of the e-learning but is modified to be more applicable to the target groups therefore providing a more relevant and memorable training experience. In addition, face to face training allows concepts to be explained and expanded upon and questions can be asked to aid understanding.