Camden & Islington NHS Foundation Trust

Data protection audit report

February 2024

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 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 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.

Camden & Islington NHS Foundation Trust (the Trust) along with Barnet, Enfield, and Haringey Mental Health Trust (BEH) agreed to a consensual audit of their data protection practices, ahead of their merger. The purpose of the audit is to provide the Information Commissioner, the Trust and BEH 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, or any data protection issues or risks which affect its 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
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.
Processor, Third Party Supplier and Controller Relationship Management	Organisations have ensured there are effective relationship management controls in place with all processors and 3rd party suppliers. There are written contracts between controllers and processors including specific minimum terms outlined in the UK GDPR. The terms ensure that processing carried out by a processor meets all the UK GDPR requirements, not just those related to keeping personal data secure.

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

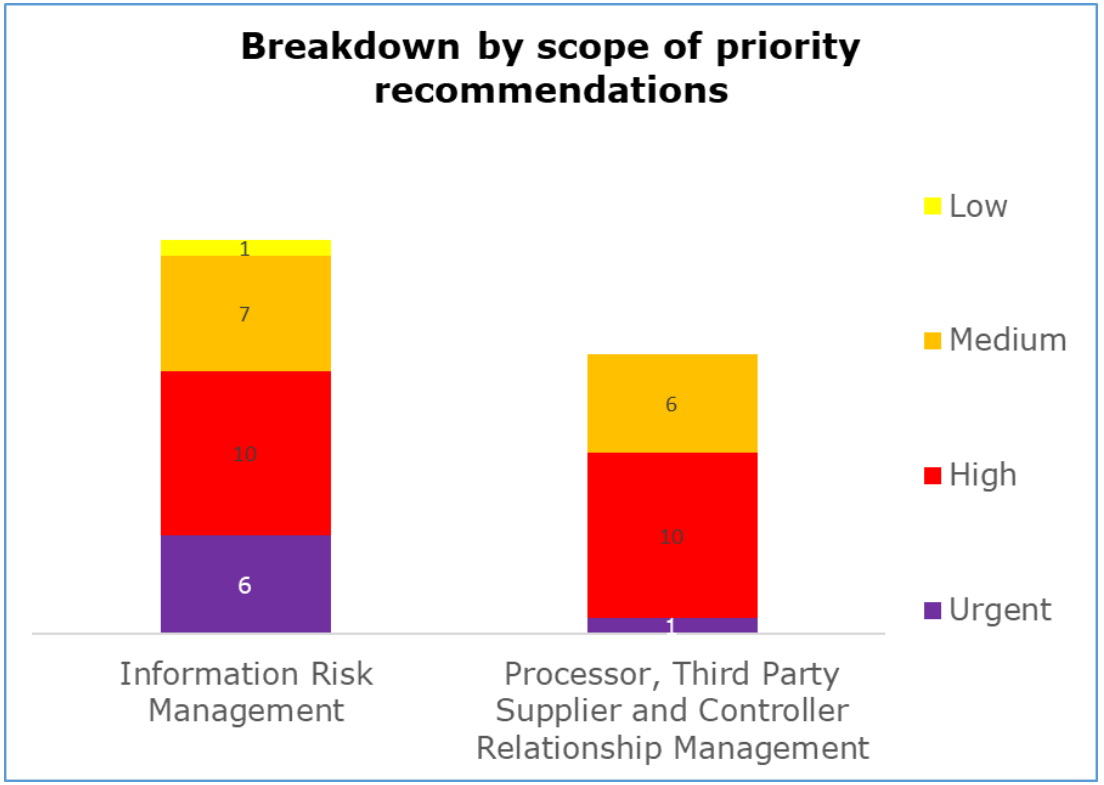
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that 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
Information Risk Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Processor, Third Party Supplier and Controller Relationship Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

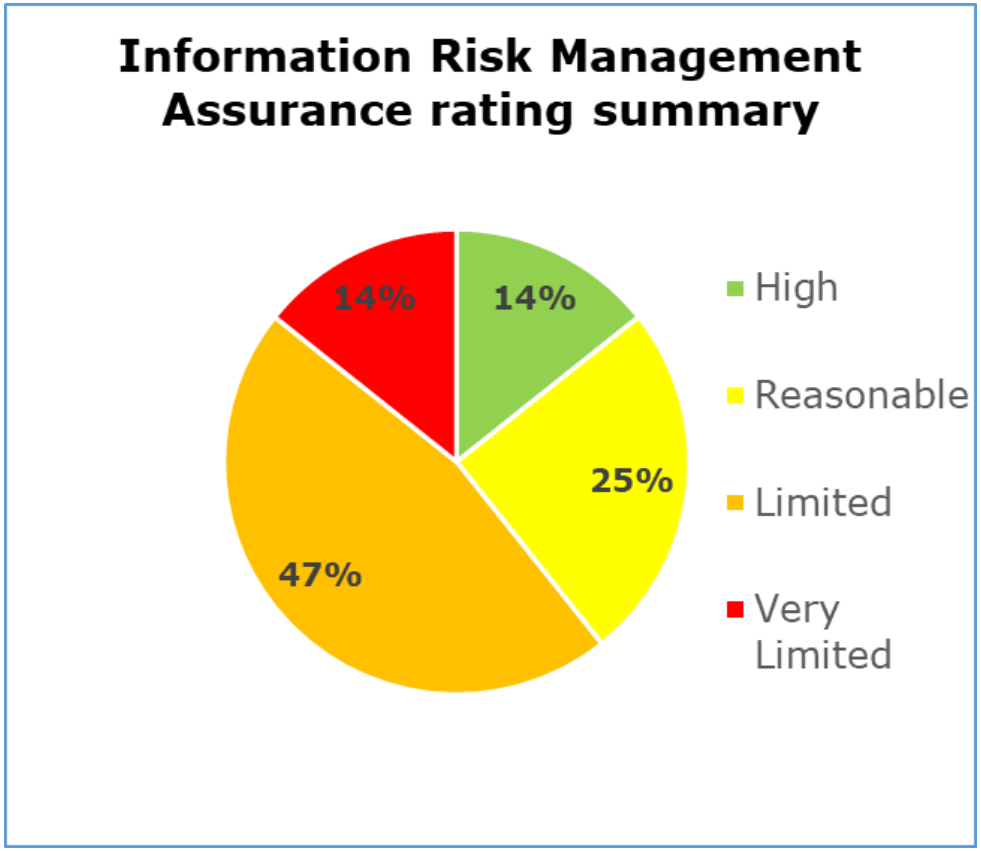
Priority Recommendations



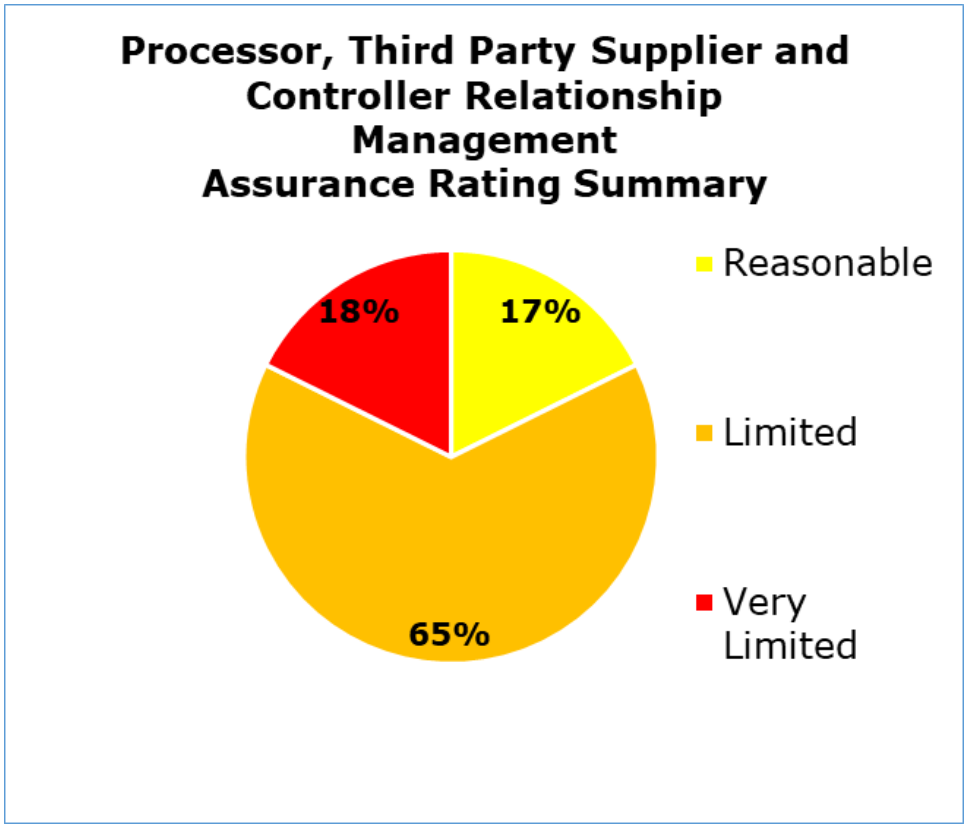
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Information Risk Management has six urgent, 10 high, and eight medium, and one low priority recommendations.
- Processor, Third Party Supplier and Controller Relationship Management has 1 urgent, 10 high, and 6 medium priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 14% high assurance, 25% reasonable assurance, 47% limited assurance, 14% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Processor, Third Party Supplier and Controller Relationship Management scope. 17% reasonable assurance, 65% limited assurance, 18% very limited assurance.

Processor, Third Party Supplier and Controller Relationship Management

Information Risk Management

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

Areas for Improvement

Information Risk Management

- Neither the DPIA policy nor the DPIA template state that processing must not take place until a DPIA has been completed and the mitigating controls have been implemented. If processing takes place prior to a DPIA, or before mitigating controls are put in place, then there is a greatly increased risk that there may be a breach as information is being processed without risk assessment or control. This may result in a breach of Article 35 of the UK GDPR.
- DPIA reviews are not being carried out. If the DPIA is not reviewed periodically, new risks may emerge which are not identified and are left uncontrolled. This may lead to a breach of Article 35 of the UK GDPR.
- Training on the responsibilities of an Information Asset Owner (IAO) has not been provided to all designated staff. Without knowledge of their responsibilities and guidance as to how to carry them out, the role of IAO cannot be adequately fulfilled.
- IAOs are not currently providing an annual assurance report to the SIRO regarding the risks around the information assets for which they are responsible.

Processor, Third Party Supplier and Controller Relationship Management

- The Trust has not formalised its approach to managing contracts with processors or 3rd party suppliers. Without a documented policy and procedure to follow, the Trust risks mismanaging the relationship with suppliers and processors, which may impede on the Trust's responsibility to ensure the security and proper use of personal data.
- The Trust Board does not currently receive any non-cyber related assurances from its suppliers and processors. Without adequate oversight of suppliers and processors acting on behalf of the Trust, there is a risk personal data is not being held securely or used in a proper manner.

- The Trust's Record of Processing Activities (RoPA) currently has missing information and is not granular enough. As such, the Trust may not currently be compliant with Article 30 UK GDPR.
- The Trust is not currently undertaking any assurance activities with processors or 3rd Party Suppliers throughout the lifetime of the contract.

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.