Barnet, Enfield and Haringey Mental Health NHS Trust

Data protection audit report

March 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.

Barnet, Enfield and Haringey Mental Health NHS Trust (the Trust) along with Camden and Islington NHS Foundation Trust agreed to a consensual audit of its data protection practices, ahead of their proposed merger.

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.

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.

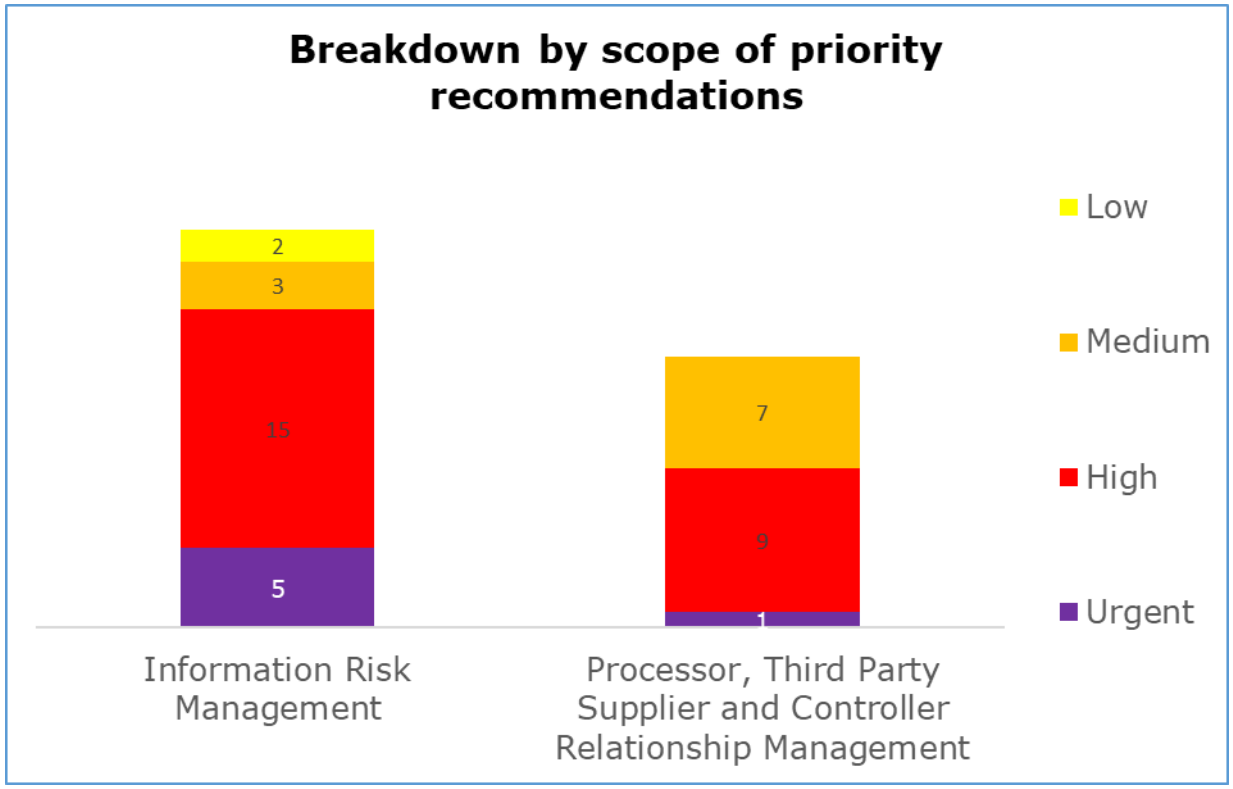
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential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

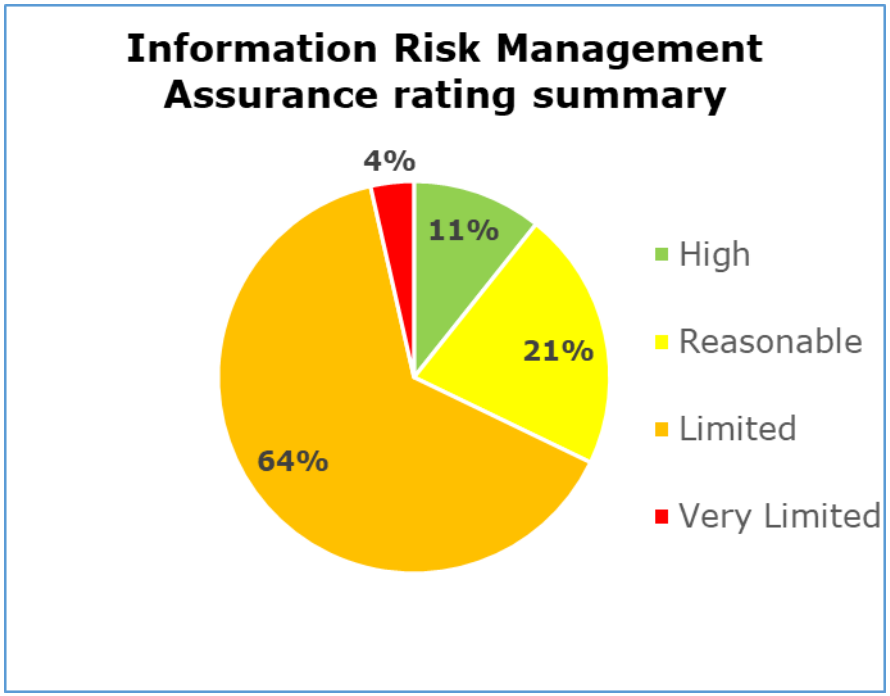
Priority Recommendations



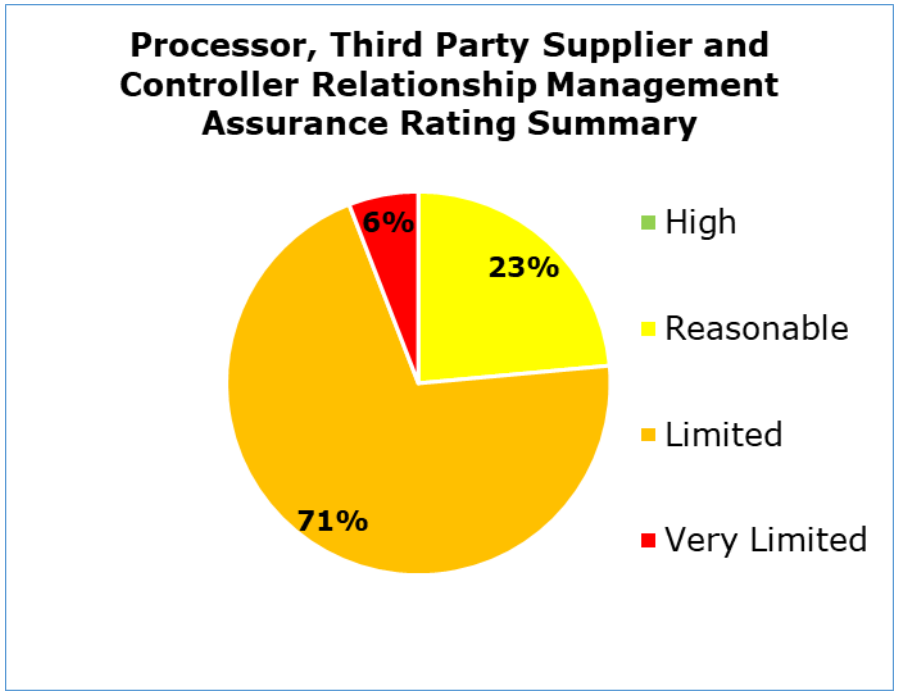
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Information Risk Management has five urgent, 15 high, three medium and two low priority recommendations
- Processor, Third Party Supplier and Controller Relationship Management has one urgent, nine high, seven medium and no low priority recommendations

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 11% high assurance, 21% reasonable assurance, 64% limited assurance, 4% 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. 0% high assurance, 23% reasonable assurance, 71% limited assurance, 6% very limited assurance.

Information Risk Management

Processor, Third Party Supplier and Controller Relationship Management

The speedometer chart 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

- Relevant policies and procedures do not state that processing should not take place before a Data Protection Impact Assessment (DPIA) has been completed and mitigating actions put in in place.
- DPIA policies and templates require review and updating so they capture enough detail to ensure that they are fully compliant with the legislation.
- Processes to deal with information risk following a data breach are not built into incident or breach management, and there is therefore a danger that risks will not be adequately controlled, leading to possible further breaches.
- The Trust has yet to put designated Information Asset Owners (IAOs) in place for all information assets so risks relating to those assets may not be adequately identified and managed.

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'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 undertaking any proactive audits with its processors to collect assurances of compliance with Article 28 UK GDPR. If the Trust has little to no assurance that data processors are complying with Article 28, it risks breaching UK GDPR Article 5(1)(f), concerning the organisational and technical measures in place to secure personal data, as well as Article 5(2).

- 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.

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