University College London Hospitals NHS Foundation Trust

Data protection audit report

April 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.

University College London Hospitals NHS Foundation Trust (the Trust) agreed to a consensual audit of its data protection practices.

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 and Cyber Security	To establish that the organisation has an effective Information Security Management System (ISMS) in place with appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of personal data and protect information processing systems and facilities from cyber security threats.
Records Management	There are processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

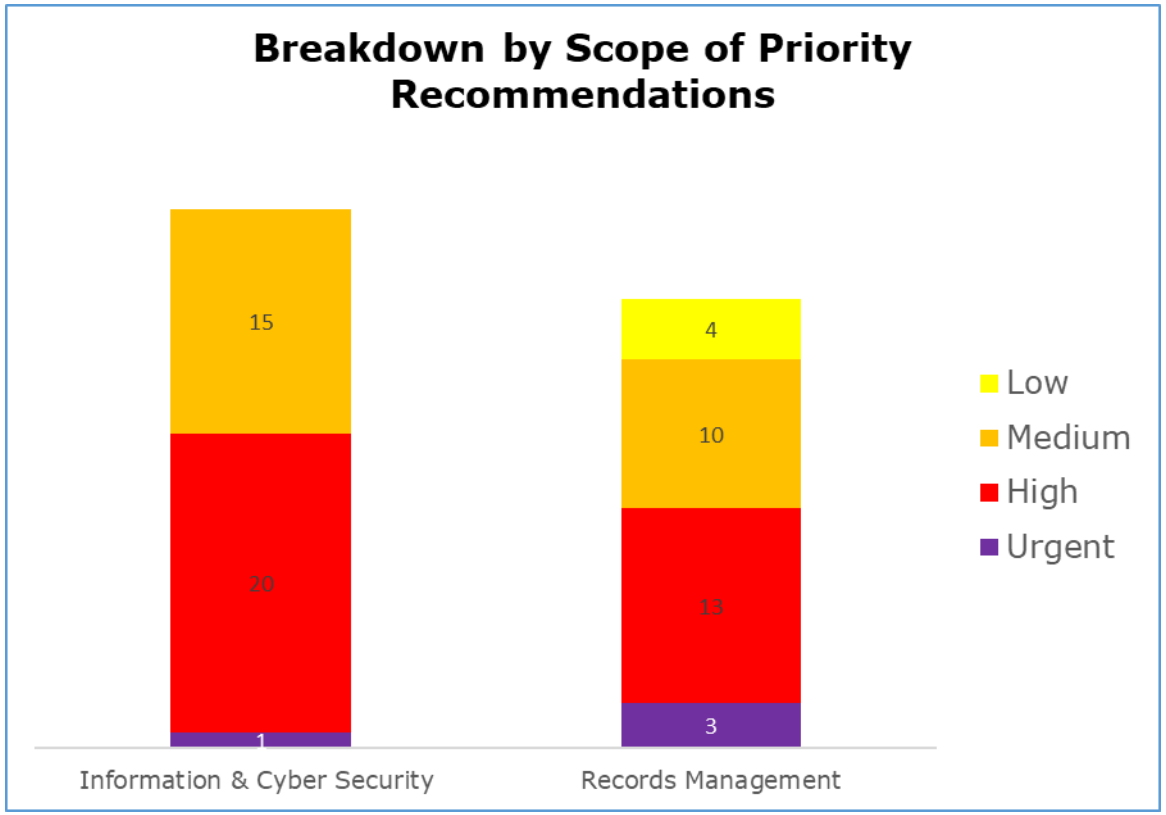
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential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

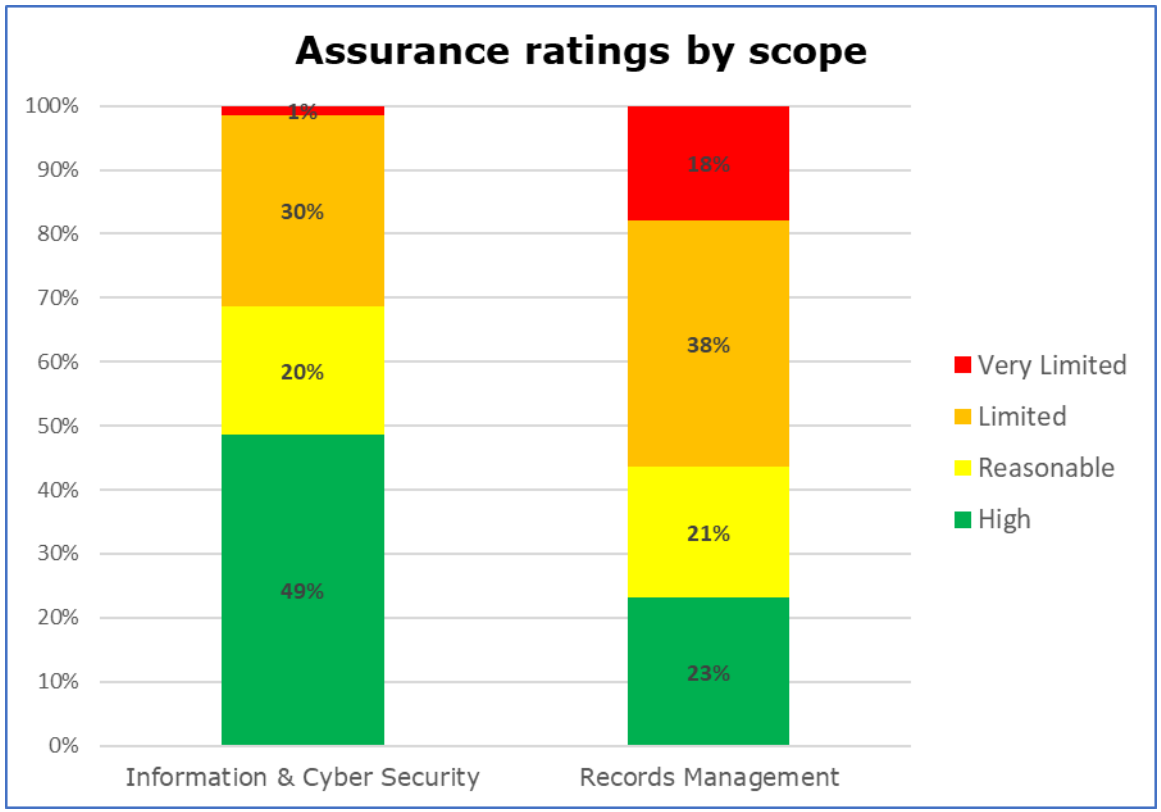
Priority Recommendations



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

- Information and Cyber Security has one urgent, 20 high, 15 medium and no low priority recommendations.
- Records Management has three urgent, 13 high, 10 medium and four low priority recommendations.

Graphs and Charts



The bar chart above shows a breakdown by scope area of the assurance ratings assigned to each control:

- Information and Cyber Security had 49% of controls rated as having high assurance, 20% reasonable assurance, 30% limited assurance and 1% very limited assurance.
- Records Management had 23% of controls rated as having high assurance, 21% reasonable assurance, 38% limited assurance and 18% very limited assurance.

Areas for Improvement

Information and Cyber Security

- The Trust should ensure their approach to the use of removeable media is updated to reflect current security standards and utilise current security techniques. Documentation should be regularly reviewed to ensure it remains fit for purpose and considers developments in security requirements.
- The Trust should ensure information security classification labelling is implemented and followed across the organisation. Supporting procedures should be developed and disseminated to all staff.
- The Trust should improve its practices around the ongoing review of standard and privileged user accounts to ensure staff only have access to systems and applications at the appropriate level they need to perform their current role. There is also an opportunity to implement stronger controls and operational processes so that all user access is disabled in a timely manner when someone leaves the Trust.
- The Trust should ensure there are documented business continuity/disaster recovery (BC/DR) plans across all areas of the organisation, which are subject to regular review and testing in line with the importance of the information assets they relate to. Relevant staff should be adequately trained and prepared so they can competently perform designated technical and functional roles if BC/DR plans are implemented in response to an adverse event.

Records Management

- The Trust's record of processing activities (ROPA) does not contain all information required under UK GDPR article 30 and is not subject to regular updates. Furthermore, The Trust does not conduct regular information flow mapping exercises, and therefore they may not have an accurate picture of how information is being processed within the Trust.

- The Trust has no formalised internal audit programme nor undertakes third party audits, which review the security of Trust records storage.
- The Trust is not disposing of records in line with the retention schedule and, therefore, is not complying with the 'storage limitation' principle as outlined in UK GDPR Article 5(1)(e).

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