King's College Hospital NHS Foundation Trust

Data protection audit report

August 2023

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 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.

The purpose of the audit is to provide the Information Commissioner and King's College Hospital NHS Foundation Trust (KCHFT) with an independent assurance of the extent to which KCHFT, 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 KCHFT's processing of personal data. The scope may take into account any data protection issues or risks which are specific to KCHFT, identified from ICO intelligence or KCHFT'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 KCHFT, the nature and extent of KCHFT's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to KCHFT.

It was agreed that the audit would focus on the following areas.

Scope area	Description
Requests for Access and Data Portability	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.
Personal Data Breach Reporting & Management	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate
Information Risk Management	The extent to which the organisation has applied a "privacy by design" approach, manages information risks 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.

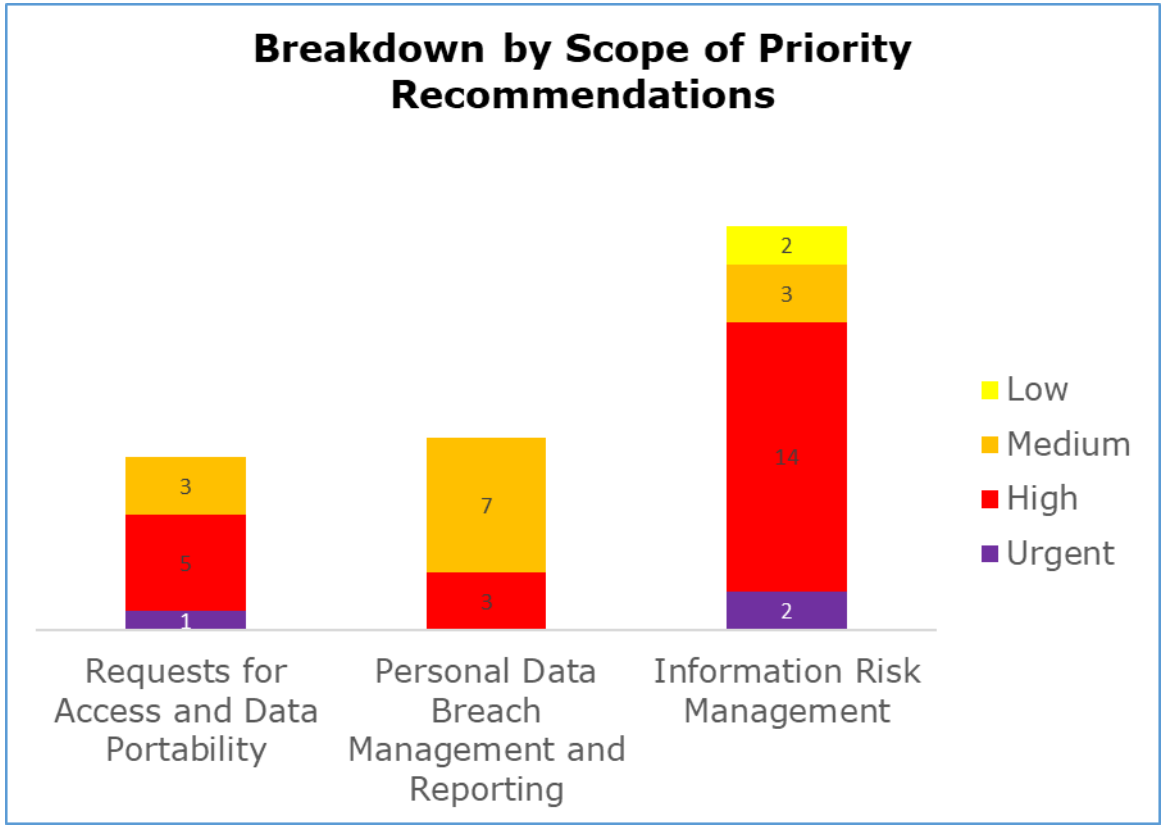
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential 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 KCHFT 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. KCHFT'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
Requests for Access and Data Portability	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.
Personal Data Breach Management & Reporting	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.
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.

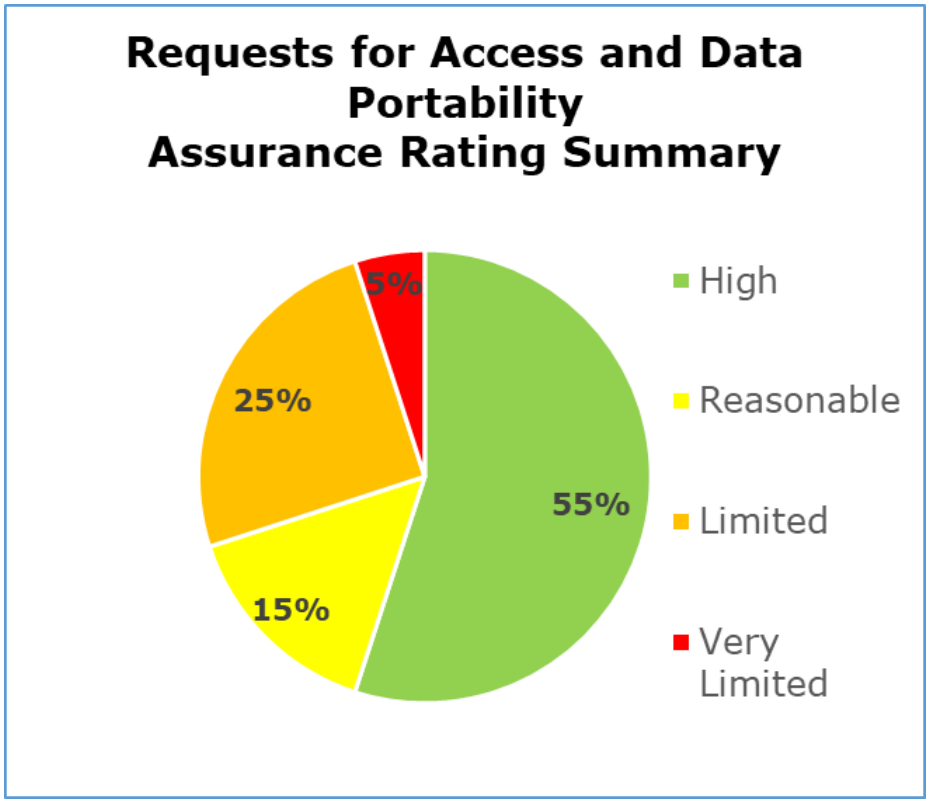
Priority Recommendations



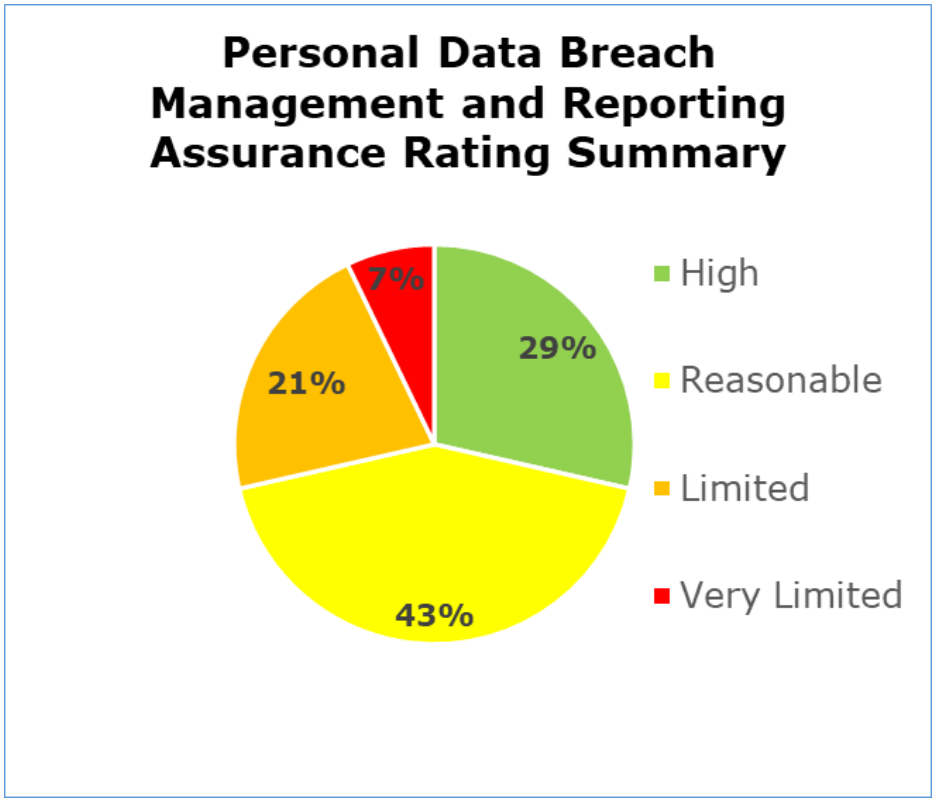
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Requests for Access & Data Portability has 1 urgent, 5 high and 3 medium priority recommendations.
- Personal Data Breach Management & Reporting has 3 high and 7 medium priority recommendations.
- Information Risk Management has 2 urgent, 14 high, 3 medium and 2 low priority recommendations.

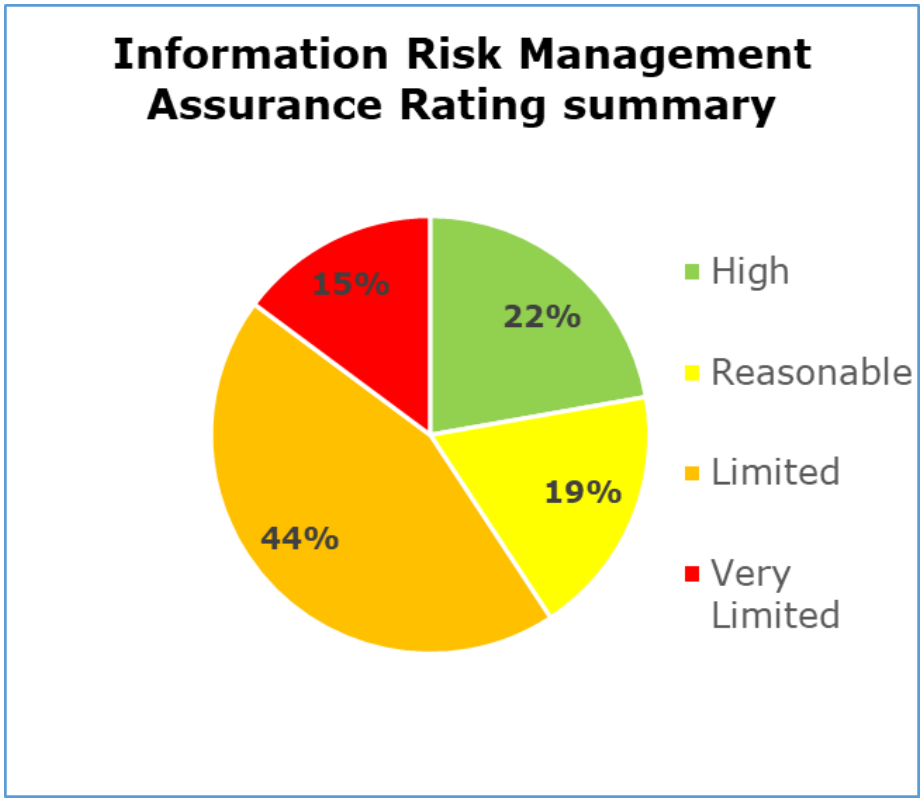
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access and Data Portability scope. 55% high assurance, 15% reasonable assurance, 25% limited assurance, 5% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management & Reporting scope. 29% high assurance, 43% reasonable assurance, 21% limited assurance, 7% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 22% high assurance, 19% reasonable assurance, 44% limited assurance, 15% very limited assurance.

Areas for Improvement

Requests for Access and Data Portability

The Trust must ensure all disclosures of patient health data are made in accordance with DPA 2018 Sch.3 Part 2 Section 6. Clinicians must have sight of proposed disclosure bundles to perform serious harm tests and request appropriate redaction of the information.

The Trust has experienced a recent drop in compliance with subject access request statutory response timescales and work needs to be done to address this issue. Further plans need to be developed to ensure the Trust is able to quickly action any drop in compliance. Such plans should be kept under constant review.

The Trust should ensure its staff are aware of the requirement to accept verbal access requests. This should be supported with clarification of the procedure for accepting and dealing with a verbal request.

Personal Data Breach Management and Reporting

The Trust should perform root cause analysis of significant personal data breaches. This will reduce the likelihood of reoccurrence of data breaches.

There should be a documented and clear process for making statutory notifications of data breaches to affected individuals to demonstrate compliance with the UK GDPR Articles 34 and 5(2).

The Trust should ensure guidance, policies and procedures are all easily accessible on the staff intranet. There should be appropriate tags associated with documents to allow easy access via the search function.

Information Risk Management

The Trust should complete an information flow mapping exercise, to ensure the information asset register accurately documents the Trust's information assets and information asset owners.

At the time of the audit, the Trust's risk management tool, InPhase, did not have the capability to create an information risk register. This facility has now been added, so the Trust should continue its work to ensure that all information risks across the Trust are being accurately recorded on InPhase.

The Trust must ensure it is performing regular reviews of data protection impact assessments (DPIAs). Without regular reviews, the Trust risks becoming unaware of new risks which have arisen during the processing. As such, the Trust may not be able to properly consider the risks resulting in a potential breach of UK GDPR Article 35.

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 KCHFT.

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