Hertfordshire Partnership University NHS Foundation Trust

Data protection audit report

September 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.

Hertfordshire Partnership University 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 area covered by this audit is 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.

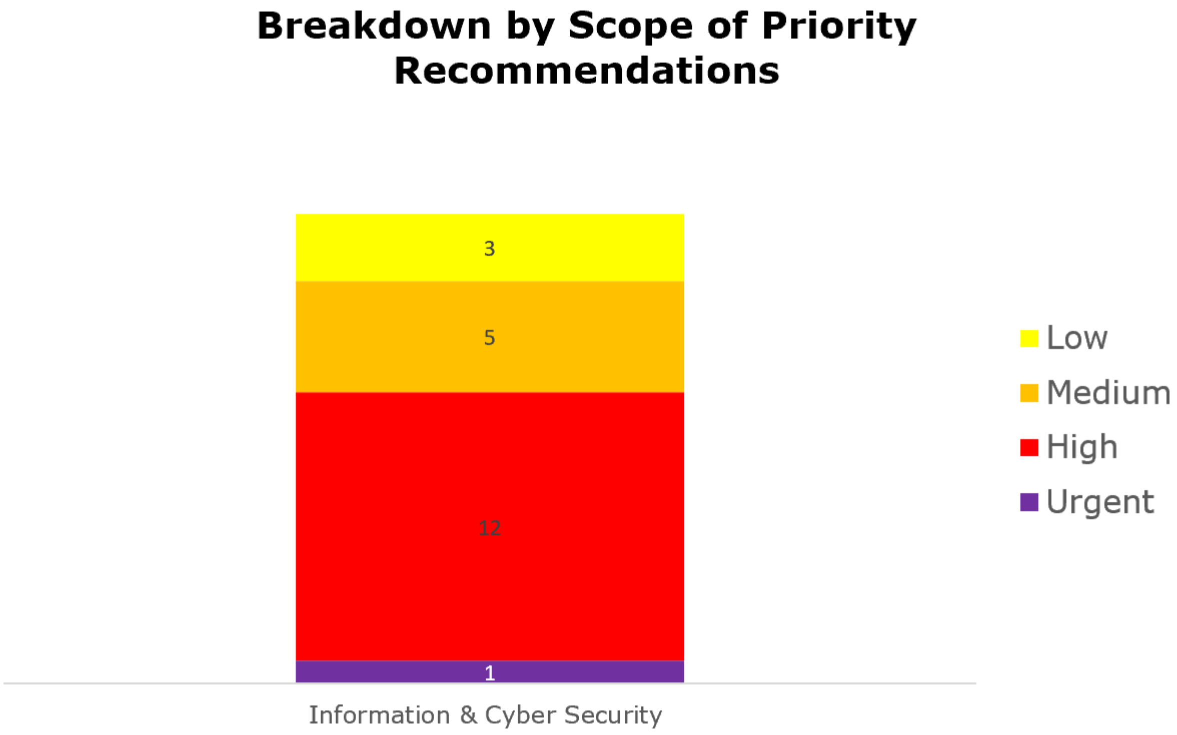
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential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

Priority Recommendations

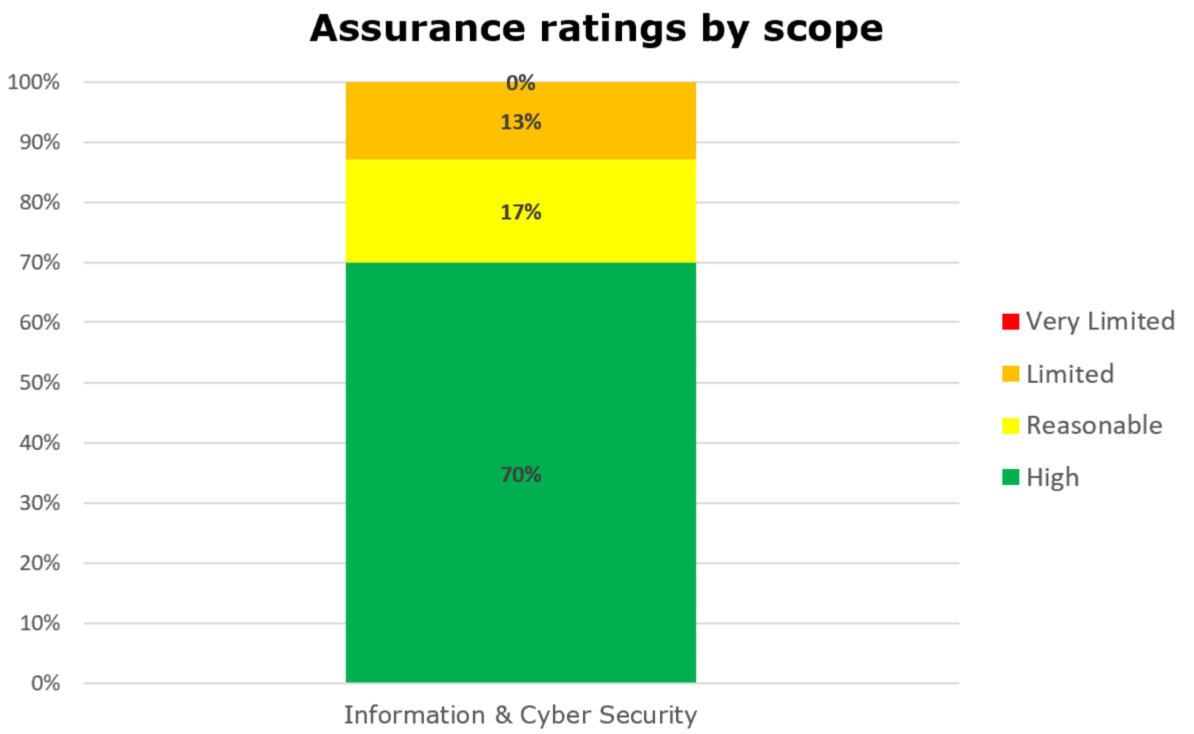


Breakdown by Scope of Priority Recommendations

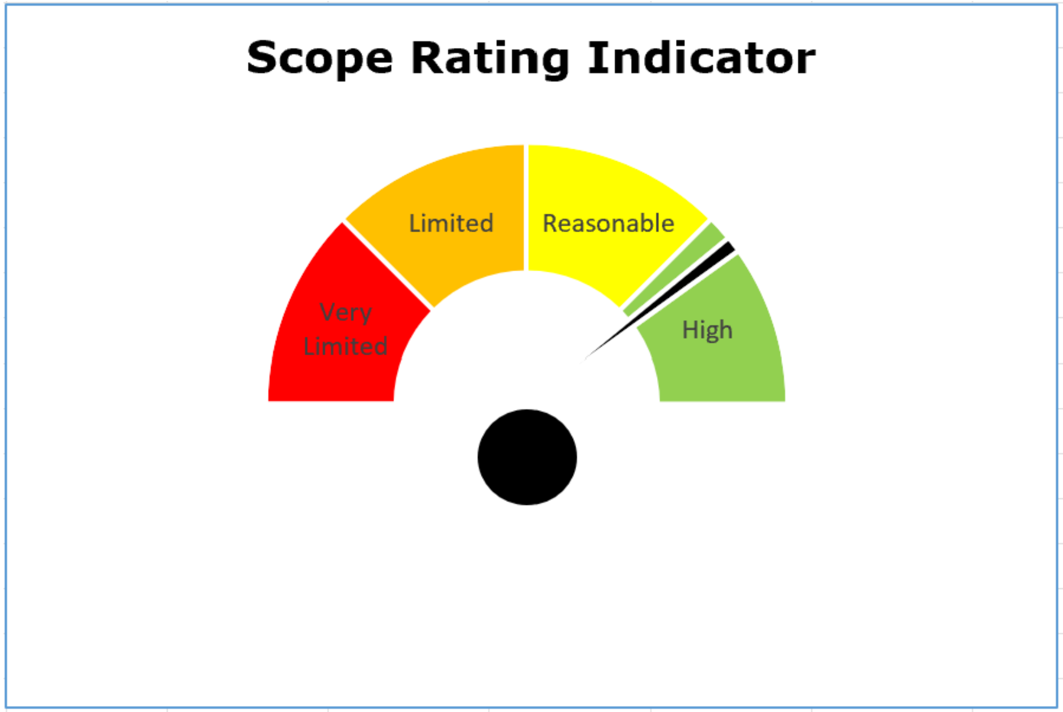
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Information & Cyber Security has one urgent, 12 high, five medium and three low priority recommendations.

Graphs and Charts



The bar chart above shows a summary of the assurance ratings awarded in the Information & Cyber Security scope. 70% high assurance, 17% reasonable assurance, 13% limited assurance, zero% very limited assurance.



The speedometer chart above gives a gauge of where Hertfordshire Partnership University NHS Foundation Trust sits on our assurance rating scale from high assurance to very limited assurance.

Areas for Improvement

Information and Cyber Security:

- The Trust has completed a number of Data Protection Impact Assessments (DPIA) however they could strengthen their risk assessment process by conducting regular reviews of existing DPIAs so that they have assurance that they remain relevant in the event of a substantial change to the nature, scope, context or purposes of the processing, and that all information risks in ongoing systems have been identified and mitigated.

- The Trust's information asset register is in the process of being updated and improved. The Trust should ensure that the register is completed and embed a comprehensive network of Information Asset Owners and Administrators- all of whom should receive training to ensure the assets are regularly and accurately risk assessed and reviewed.

- The Trust has an overarching business continuity plan which is supplemented by specific team level plans. Currently not all team plans have been completed and signed off. Without comprehensive, robustly tested plans in place, the Trust may fail to recover in the event of a major incident, and personal data may be lost or made vulnerable as a result.

- The Trust should formalise, in policy, a standard approach to reviewing system user access to ensure this is done in a consistent, accurate way. Without regular, mandated review, cases of inappropriate access may not be detected.

Best Practice

- Trust policy documents contain a ‘document on a page' on the first page which says briefly why staff need to know about the policy, and gives three key messages. This concise delivery of key messages, makes the policies as a whole clear and accessible to staff who may need to consult with it ‘at a glance’.

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