Portsmouth Hospitals University NHS Trust

Data protection audit report

May 2022

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.

Portsmouth Hospitals University NHS Trust (the Trust) agreed to a consensual audit of their 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 of this audit was 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, 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 the scope area to take into account the organisational structure of the Trust and the nature and extent of the Trust's processing of personal data. 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
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

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

However, due to the outbreak of Covid-19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, the Trust agreed to continue with the audit on a remote basis. A desk-based review of selected policies and procedures and remote telephone interviews were conducted from 25 to 27 April 2022. The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

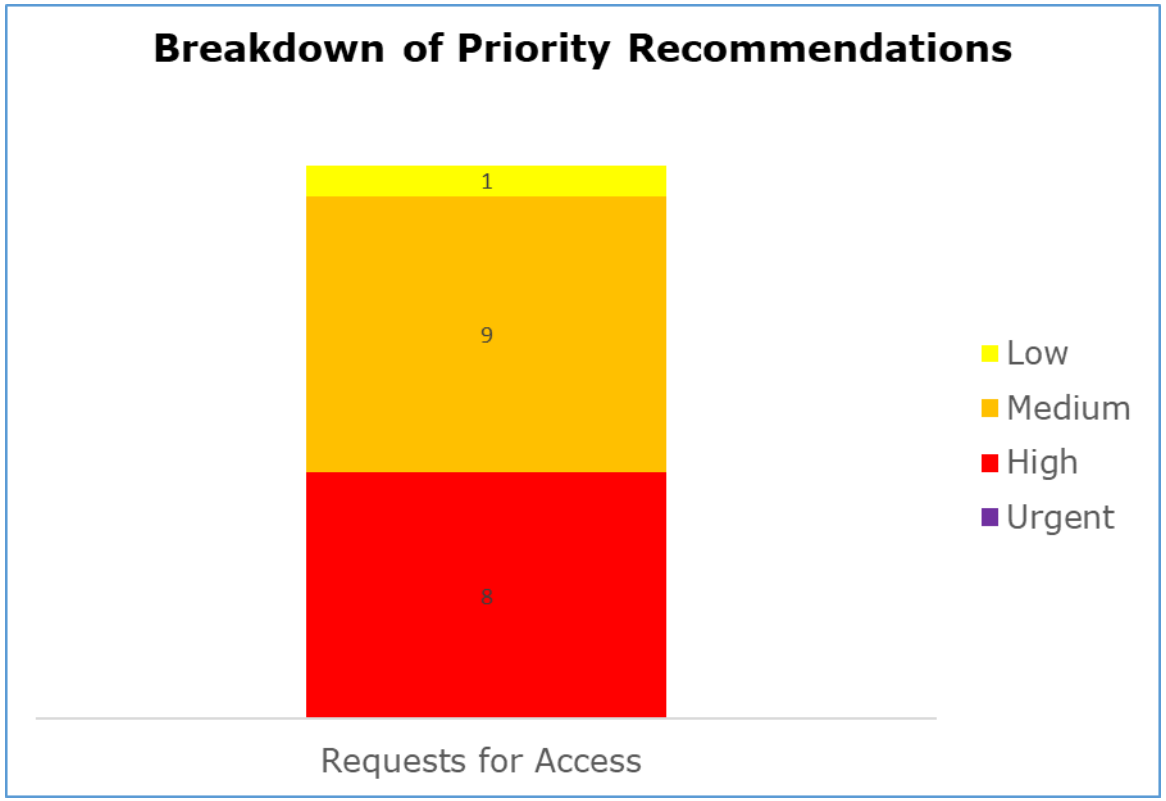
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that 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
Requests for Access	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.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

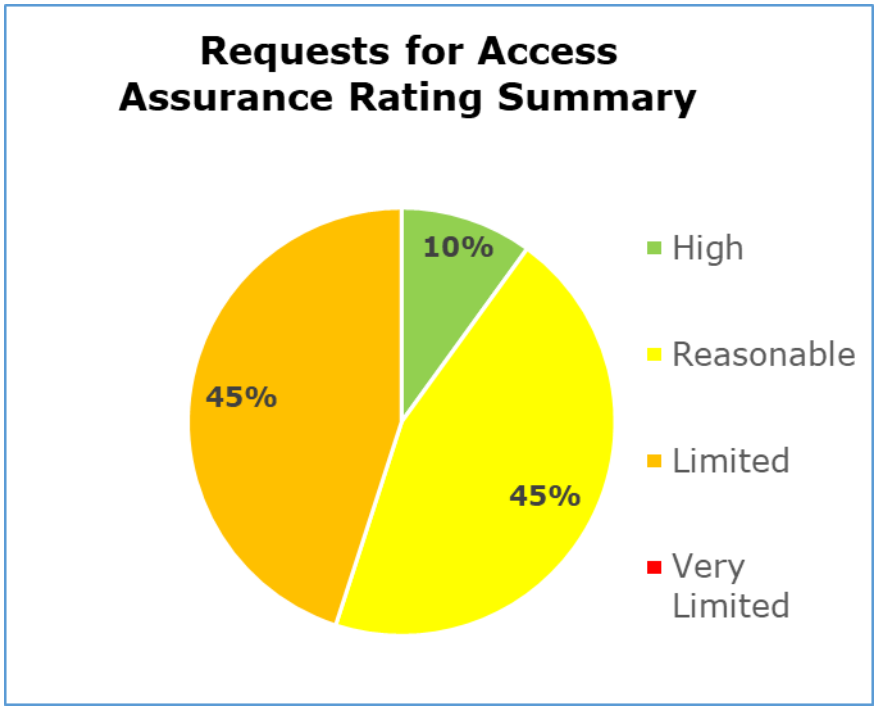
Priority Recommendations



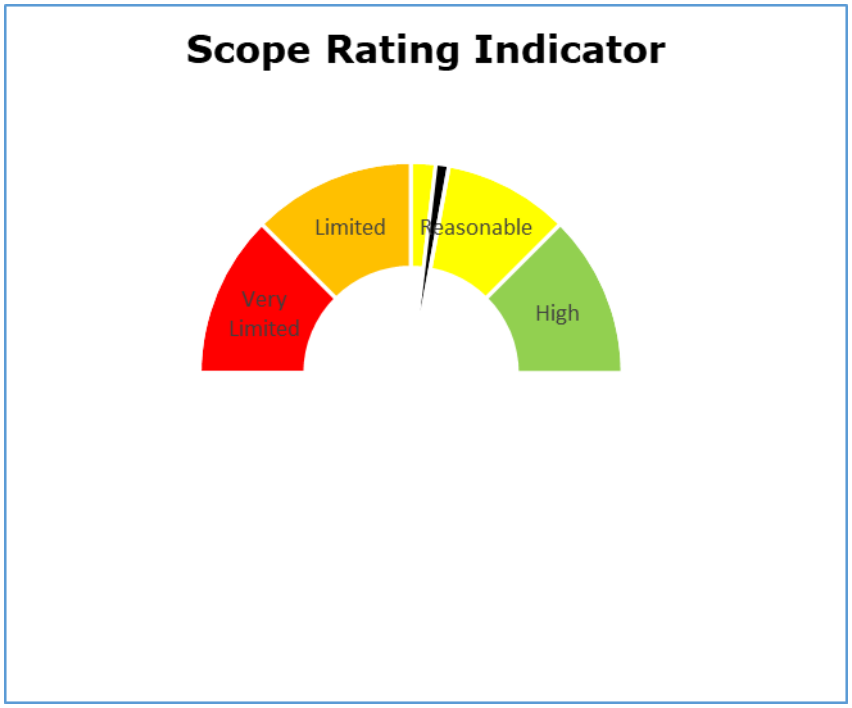
The bar chart above shows a breakdown of the priorities assigned to our recommendations made.

Requests for Access has 0 urgent, 8 high, 9 medium and 1 low priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 10% high assurance, 45% reasonable assurance, 45% limited assurance, 0% very limited assurance.



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

- The Trust's main subject access request (SAR) policies, procedures, staff guidance and training materials should be improved so that they fully reflect the requirements of the UK GDPR. They should be accurate, sufficiently detailed, aligned with each other and cover the handing of both written and verbal SARs made to the Trust.
- Additional appropriate training should be provided to all staff to help them identify and channel written and verbal SARs effectively. There is also a need to deliver additional ongoing specialist training to staff that are involved in the actual handling of SARs.
- The guidance that the Trust makes available to data subjects to help them make valid SARs should be improved so that it is easy to locate and can be understood by all individuals, including those with additional needs and those who do not have access to the internet.
- Records management procedures and working practices concerning manual records that contain personal data should ensure that such records can be easily located in a timely manner so that the Trust is able to respond to SARs within statutory time limits.
- Improvements to the Trust's processes and working practices, as well as the adequate allocation and resilience of staffing resources, should help the Trust in meeting statutory response time limits in relation to employee SARs.

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