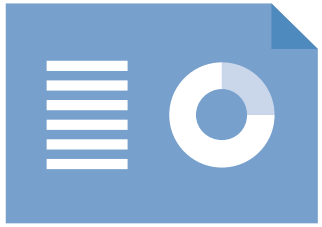
Frimley Health NHS Foundation Trust

Data protection audit report – Executive Summary

November 2019

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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 sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The purpose of the audit is to provide the Information Commissioner and Frimley Health NHS Foundation Trust (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 Trust agreed to a consensual audit in July 2019. It was agreed that the audit would focus on the following area(s):

Scope Area	**Description**
Requests for Personal Data & the Right To Rectification	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data. There are appropriate procedures in operation for recognising and responding to individuals' requests for rectification of their personal data.

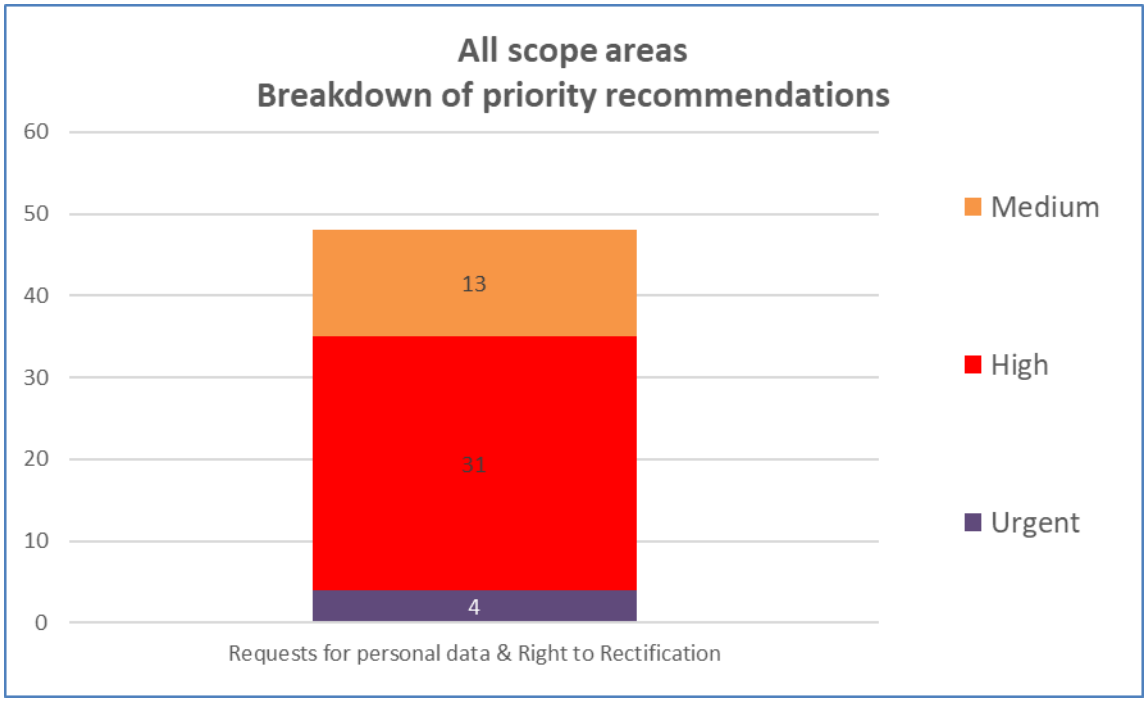
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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 Personal Data & Right to Rectification	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.

Priority Recommendations



Areas for Improvement

The Trust should ensure that it enhances awareness for all SAR handlers around exemptions and what could constitute identifiable third party data so that potential redaction and exemption cases are not inadvertently disclosed. Personal data held about patients that originated outside the Trust should also be included in responses (subject to redaction and exemption checks).

The Trust should ensure that key steps in the SAR handling process, including reviews of responses (both before and after disclosure) are formally evidenced throughout as part of its governance audit trail.

The Trust needs to ensure that it is fully transparent to the public in terms of how they may make requests either for access or for rectification of their personal data.

The Trust should also ensure that it has mechanisms in place at outlying Trust locations to ensure that mis-directed postal requests are sent straight to the SAR team without delay in order to minimise the risk of timescale breach.

The Trust should also ensure that it records the receipt date for requests as the date they are first received into the Trust and not the first date they are received by the AHR or IG teams for processing.

Good Practice

The Trust has developed an online SAR form which, when completed by the requester, can be read straight into the RFI system. This facilitates standardisation of the request format and in itself can help to speed up processing.

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 Frimley Health 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.

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