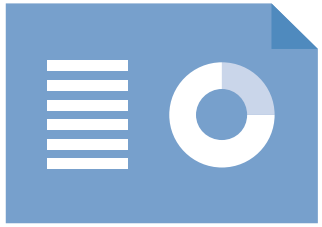
Blackpool Teaching Hospitals NHS Foundation Trust

Data protection audit report– Executive Summary

April 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 Blackpool Teaching Hospitals 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.

Blackpool Teaching Hospitals NHS Foundation Trust agreed to a consensual audit in December 2018. It was agreed that the audit would focus on the following area(s):

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Records Management	The 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.
Requests for Personal Data	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

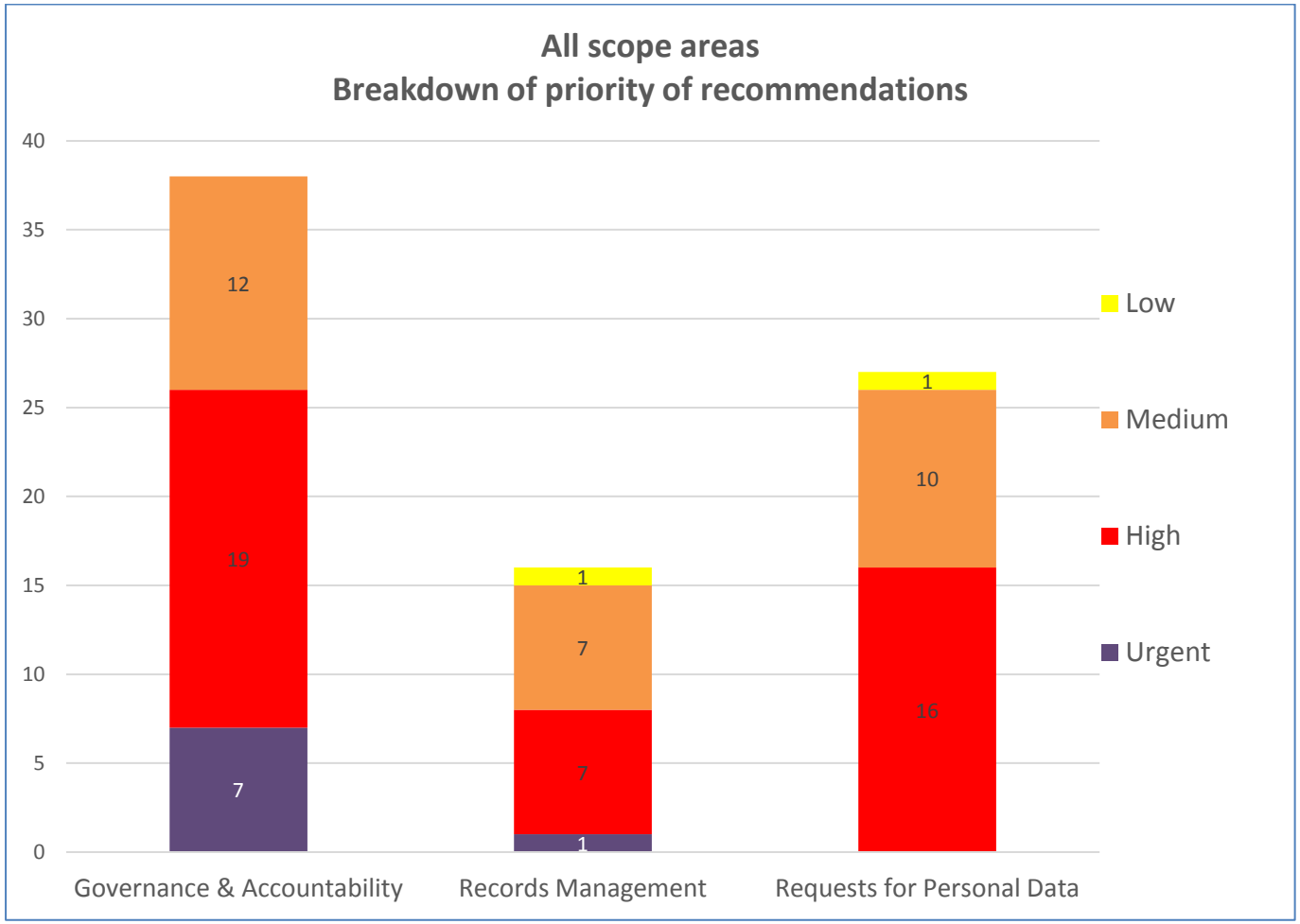
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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.

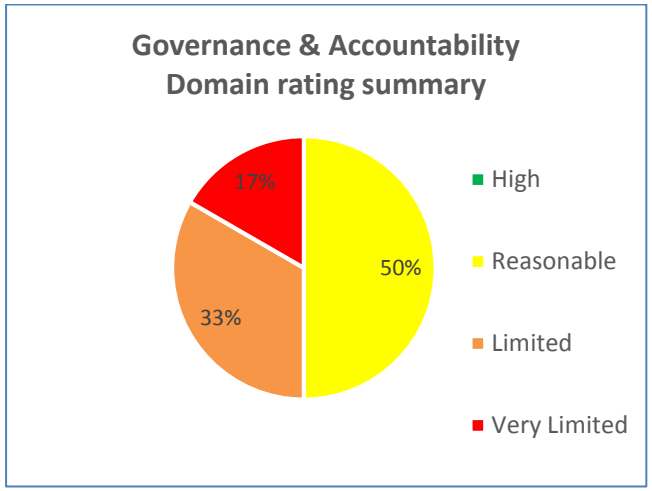
Audit Summary

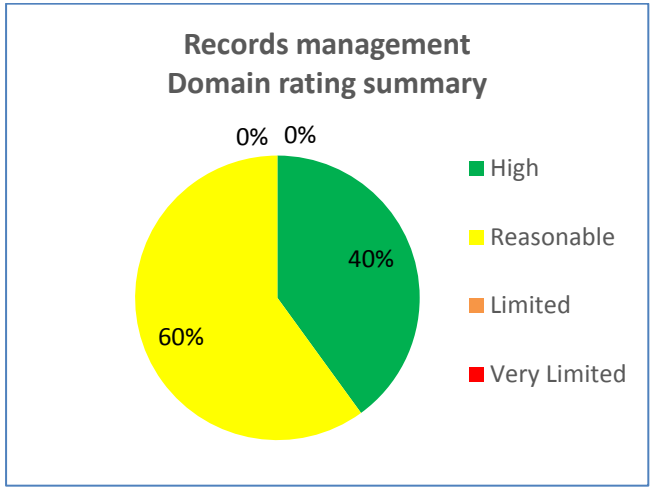
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records management	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.
Requests for personal data	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



Graphs and Charts





Areas for Improvement

The Trust has made progress on its Information Asset Register; however, it has yet to complete this work and its data flow mapping has also not been completed yet either. A full identification of processing activities is mandatory under Article 30 of the GDPR.

The Trust also needs to fully assure itself that GDPR-compliant clauses are in place with all third party processors and implement controls to actively monitor compliance with those.

The Trust has fair processing information in place for its core adult service users, but needs to ensure that fair processing information is available for all groups whose data it processes [including children and others] and also ensure that all of its processing activities are clearly linked to a lawful basis for processing.

In addition to achieving toolkit compliance on mandatory training, the Trust also needs to ensure that all staff that process SARs around the Trust receive specific GDPR training. Statutory deadlines, procedures and SOPs around SAR processing need to be extensively documented and formalised throughout.

The Trust should maintain a clear governance audit trail by formally evidencing the outcomes of SAR performance reviews [including breaches] and ensure that there is good, documented communication with the data subject throughout the process.

Good Practice

It was reported that a TV game show simulation and a live cyber-attack visual feed had been used to increase staff awareness and engagement. We were pleased to hear that the Trust has developed creative ways of raising awareness around data protection.

The Trust has invested in an on-site industrial size shredder which processes all paper at the Blackpool site, thereby helping to minimise the risk presented by mishandling or misclassification of confidential waste paper.

Whilst still in various stages of completion, refinement and user-testing, we were also very encouraged to see the in-house development of a number of digitised workflows and applications to support IG and to hear of the proposals to eventually integrate them at a later stage.

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