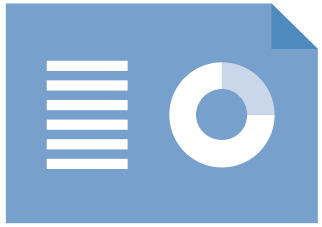
Bridgewater Community Healthcare NHS Foundation Trust

Data protection audit report

March 2020

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.

Bridgewater Community Healthcare NHS Foundation Trust (the Trust) has agreed to a consensual audit by the ICO of its processing of personal data. An introductory meeting was held on 14th November 2019.

Telephone interviews were conducted prior to the onsite visit. The audit fieldwork was undertaken at The Trust's site in Birchwood on 11 – 13 February 2020.

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.

It was agreed that the audit would focus on the following area(s):

Scope Area	Description
Governance and 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.
Personal Data Breach Management and Reporting	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.

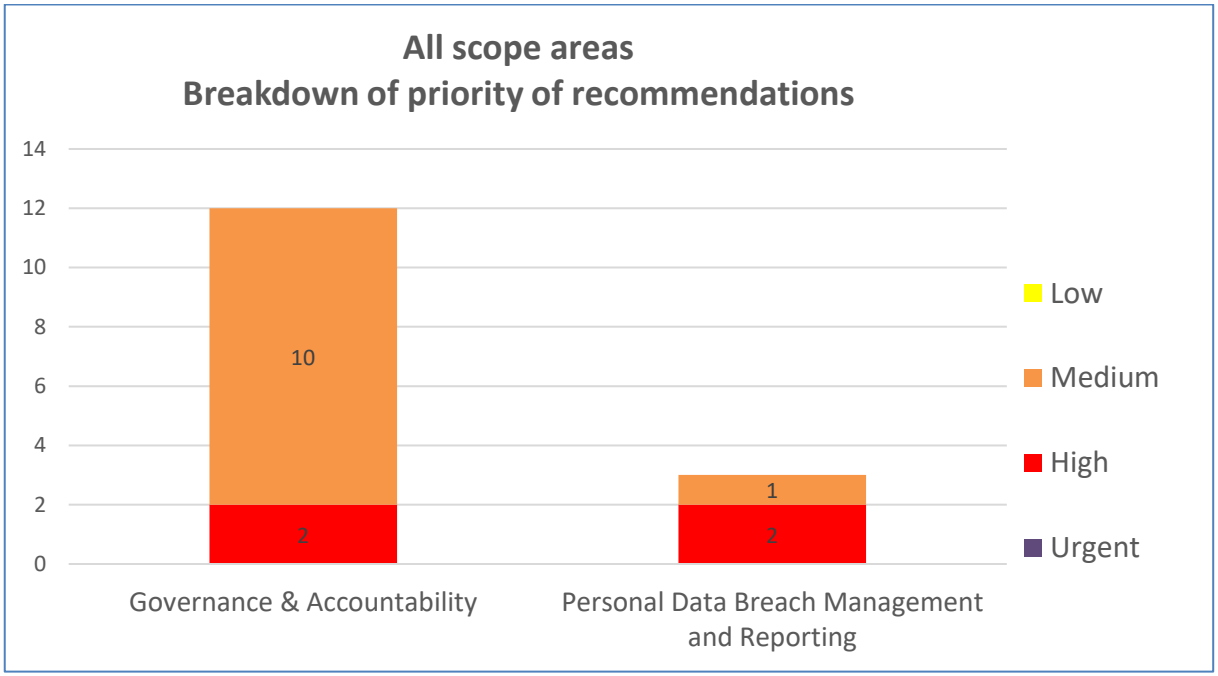
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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	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.
Personal Data Breach Management and Reporting	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



Areas for Improvement

Governance and Accountability

Privacy Notices published should cater for all service users and particular care should be made in recognising young people's data protection rights.

Lawful basis for processing needs to be clearly identified and defined as part of the record of processing activities.

Processor contracts should have the necessary clauses defined to give the Trust assurance that data protection legislation obligations are met, particularly in terms of information security, data protection training and incident management.

Personal Data Breach Management and Reporting

Procedures in place to notify individuals when they have been subject to a data breach need to be formalised. Key information in regards to contact details, measures taken and name of the supervisory authority need to be shared with individuals.

Best Practice

The Information Governance audit on Data Protection Awareness demonstrates a commitment to ensuring key IG messages are filtering through to all staff and actions, where gaps are highlighted, are addressed and discussed at DIGIT meetings.

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