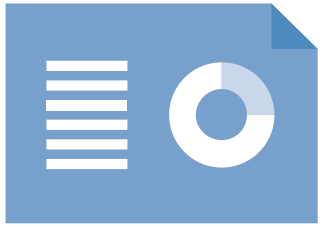
Berkshire Healthcare NHS Foundation Trust

Data protection audit report

May 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.

Berkshire Healthcare NHS Foundation Trust (the Trust) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 8TH January with representatives of the Trust to discuss the scope of the audit.

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.
Cyber Security	The extent to which the organisation has technical and organisational measures in place to protect personal data from external and internal attacks on confidentiality, integrity and availability.

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.

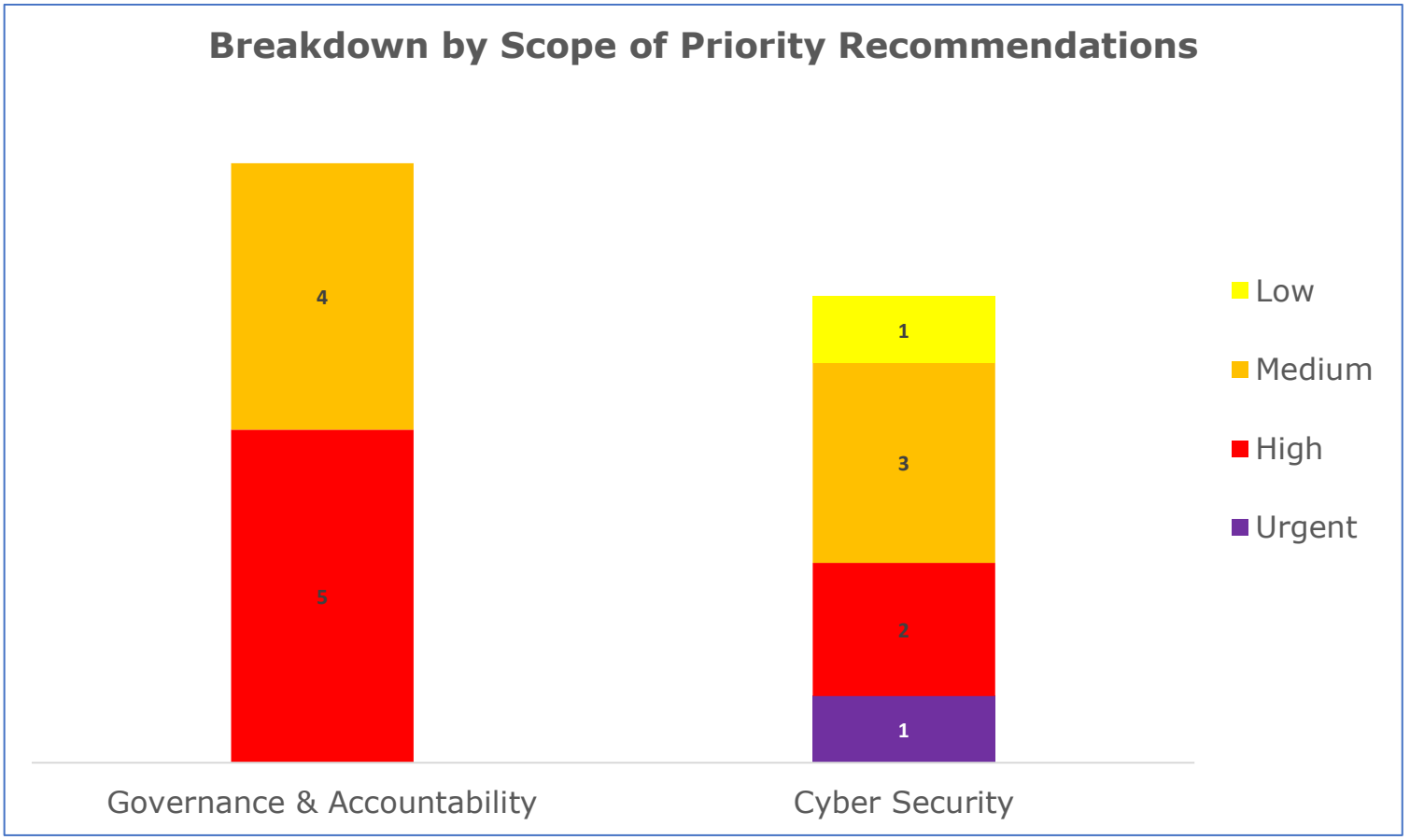
However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore the Trust agreed to continue with the audit on a remote basis. As the Trust responded to mounting Covid – 19 pressures, auditors worked with representatives of the Trust to adapt a flexible work around to complete the audit. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 6th – 23rd April 2020. 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
Governance and 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.
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



Areas for Improvement

Governance and Accountability

To strengthen its information governance assurance programme, the Trust should now look to how it can effectively use internal risk based audits. It should devise an annual schedule of audits and add the findings of these to its information governance reports to be shared with senior management committees.

As required by schedule 1 of the DPA 2018, the Trust should ensure that it has an Appropriate Policy Document in place that is sufficient to fulfil this requirement and accurately determines the lawful basis for processing special category data.

Privacy Notices published should cater for all service users. The Trust should consider how to actively target a privacy notice to children similar to the one used for vulnerable groups.

Cyber Security

The Trust is not proactively auditing or analysing the effectiveness of its policy on records management by utilising the electronic logs available from RIO. By ensuring this is happening regularly, the Trust can gain assurance that its records system, which hold the bulk of patent data, is being accessed by staff for legitimate purposes only.

The Trust should accurately ascertain which mobile apps are used within the Trust and for what purpose. It should then closely monitor the use of these, to ensure that personal identifiable information isn't being captured or transmitted against Trust policies.

The Trust should review its use of removeable media to ensure it is properly controlled and accounted for. An asset register detailing a full inventory of removable media in use and ownership should be maintained with

regular checks to confirm accuracy. Endpoint controls should be secured or controlled to prevent unauthorised or inappropriate use.

The IM&T Teleworking Policy should be finalised and ratified as soon as possible once the technical issues highlighted have been addressed.

Best Practice

The Trust has a robust framework of management structures and policies underpinning its approach to data protection. There is a strong culture and commitment to privacy evident particularly through its DPIA process. Each DPIA includes a comprehensive screening questionnaire which considers key information security requirements.

The Trust has invested in extra training for all board members to ensure that they have the necessary skills and understanding to ensure current and emerging cyber security threats are well understood and will recognise the steps that need to be taken to mitigate the risks.

The Trust ensures that in addition to regular penetration (pen) testing, any new system that is brought online is also pen tested before it is fully signed off as fit for purpose and the results and actions are well documented. Additional pen tests are also employed on systems containing highly sensitive information.

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.