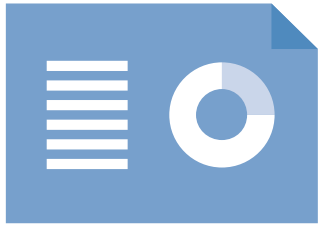
Harrogate and District NHS Foundation Trust

Data protection audit report

December 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 ICO approached Harrogate and District NHS Foundation Trust (the Trust) in June of 2019 and suggested the potential benefit of an audit. The Trust welcomed the opportunity to participate in the audit and ICO auditors visited the Trust in October of 2019.

The purpose of the audit is to provide the Information Commissioner and Harrogate and District NHS Foundation 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
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.
Personal Data Breach Management	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.
Business Continuity	The extent to which the organisation has measures in place to ensure that personal data and data subjects are not adversely affected in the event of significant functional impacts on the organisation.

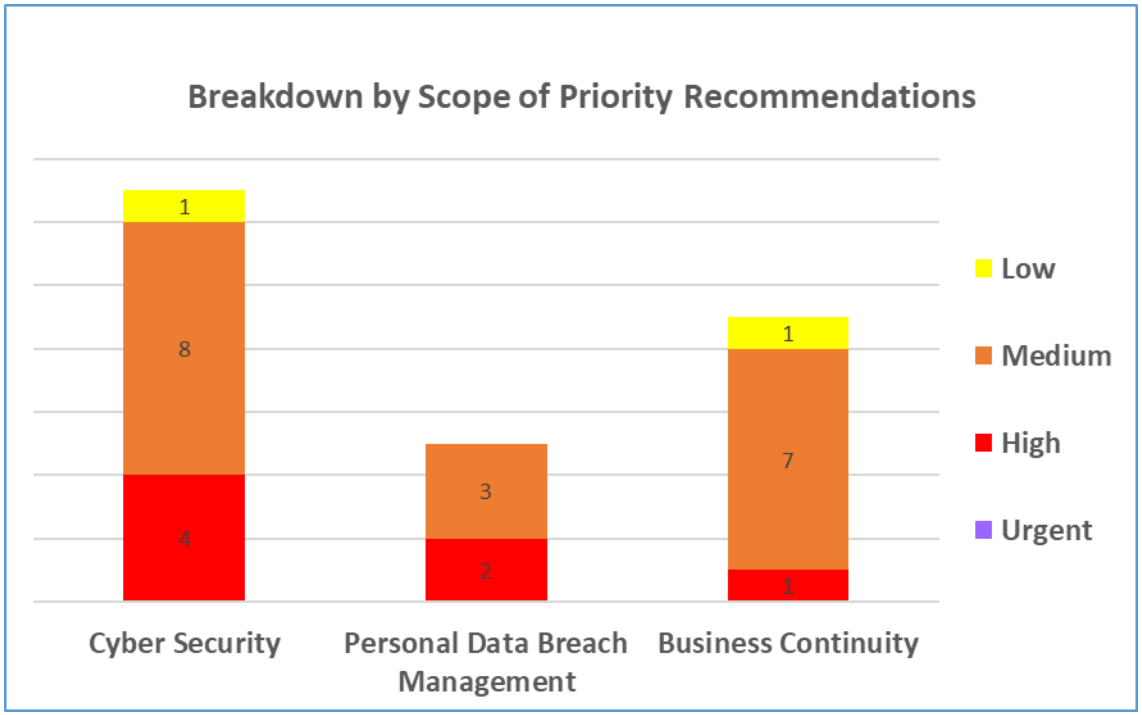
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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. Harrogate and District NHS Foundation 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
Cyber Security	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.
Personal Data Breach 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.
Business Continuity	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

Cross scope:

- Across the three scope areas the Trust has core documentation in place and auditors observed commonly understood operational processes that were being followed, however it was acknowledged that documented standard operating procedures and some key policies were absent or still under development. Examples include server build documentation, change management action plans and a user friendly acceptable use policy.

Cyber-security

- The Trust's main authentication process is through Active Directory and all staff must login through this portal before they are able to login separately to other patient systems. Active Directory uses encryption and hashing to secure passwords. However, there was uncertainty over how passwords were stored in other patient systems. The Trust should begin a program to understand how passwords are stored on those internal patient systems and regularly review the algorithms in use to ensure they remain secure.

- The Trust does not currently have a corporate policy on log retention in place. The Trust should review their approach to electronic log retention to understand how long they are retaining access logs, and the purposes for holding them. This will allow the Trust to create an organisation wide policy for electronic log retention across all of their systems that will allow full investigations of any security incidents or concerns and long term analysis of trends.

- The Trust has a robust approach to managing USB devices with effective endpoint control and a system to issue encrypted devices to users through their departments. The Trust has no mechanism in place to ensure that USB devices are returned to the issuing IT department once the user no longer has a need for them. This will ensure the Trust is able to account for the lifecycle of the device and minimise any risk of personal data being stored on them against policy and being held indefinitely by the department or the individual.

Personal Data Breach Management

- The Trust should put in place a documented procedure to notify individuals who may have been the subjects of a personal data breach and are considered to be at high risk. This should ensure that the obligations under Article 34 of the GDPR are fulfilled and that individuals are notified of at a minimum; the nature of the breach, the contact details of the data protection officer or other contact point, the likely consequences of the breach and any measures taken (or proposed to be taken) to address the breach.

- NHS organisations must submit reportable personal data breaches within 72 hours using the DSP Toolkit. The current 'Identification, reporting and management of incidents including SIRI's' policy does not clearly lay out this requirement. The Trust should ensure that guidance documents and procedures make staff aware of the obligation to report through the toolkit and the timeframe to ensure compliance with Article 33 of the GDPR.

- The Trust has not applied a retention period to breach logs retained on DATIX potentially resulting in indefinite retention. The Trust should ensure that a retention schedule is put in place considering the value of the logs, a review procedure and potential minimisation and anonymisation of personal data.

Business continuity:

- The Trust does not have any formal documentation in place demonstrating how the security of personal data will be maintained in the event of a disaster situation. The Trust should create a standard operating procedure demonstrating actions and processes that will ensure that data security remains effective during a disaster affecting the site.

- Although The Trust has a procedure in place to run a simulation test to ensure restorations of backups are effective, the frequency of the testing is not stated. The Trust should update its restoration policy to include information about the frequency of any testing of the restoration process to ensure there is an effective strategy to the testing process.

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