North Bristol NHS 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 North Bristol NHS 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 November of 2019.

The purpose of the audit is to provide the Information Commissioner and North Bristol NHS 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.

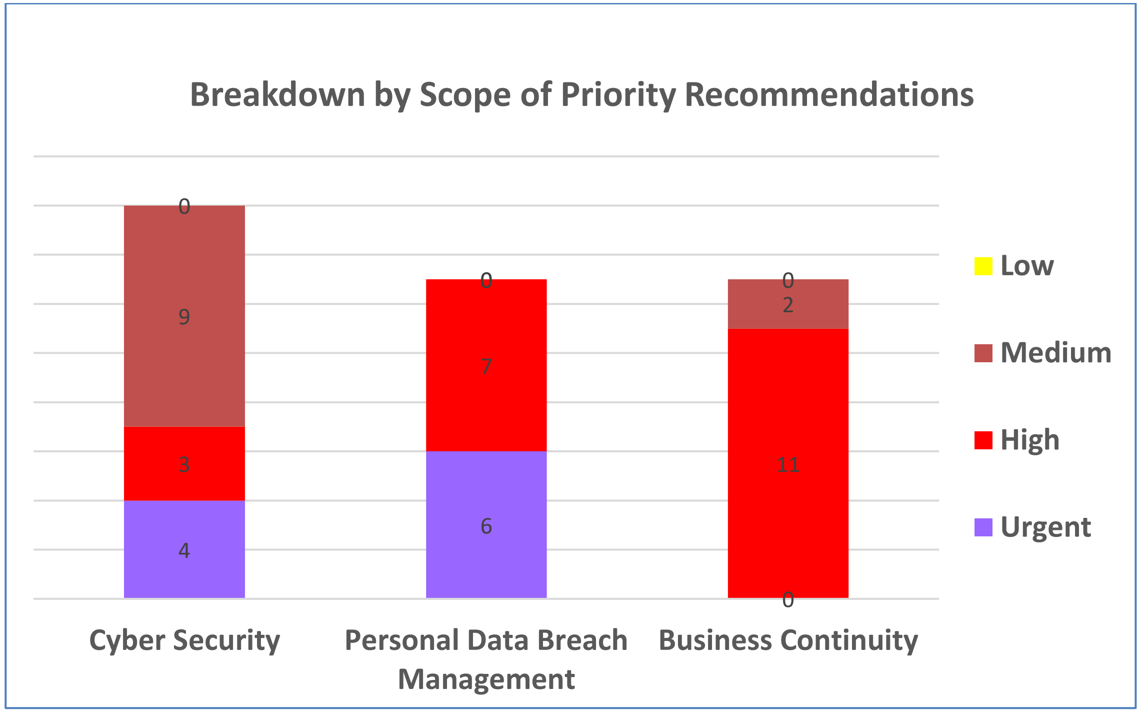
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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. North Bristol NHS 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	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Business Continuity	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations



Areas for Improvement

Cyber-security

The Trust should build in more regular reviews of its cybersecurity policies and practices to ensure compliance and to measure effectiveness in a more documented and formal basis. In particular, there needs to be a Trust wide clear desk policy with regular physical security spot checks to make sure staff are adhering to this and other measures.

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 use.

The Trust has longstanding and close working relationships with many of its key 3rd party suppliers however it needs to ensure good cybersecurity practices form the basis for all 3rd party contracts and that the Trust have documented evidence that these are included. The Trust should also carry out regular audits/inspections to gain their own assurances.

The Trust should expand their policy on log retention to ensure they are capturing the necessary data to account for all processing activities. Furthermore, any analysis should flag up breaches and/or suspicious activity in a timely proactive manner.

Personal Data Breach Management

The Trust should develop and publish emergency breach procedures and ensure that there is specific guidance on how to correctly report data breaches in Datix. It should also ensure that all breaches are entered into Datix, so that a full picture of breach risk can be formed.

The Trust should formally monitor and analyse breaches reported via Datix, to include time lags between incident dates and actual reporting and follow up on actions taken to prevent re-occurrence. Breach KPIs should be reported into senior management and any trends should inform both annual data protection training and staff awareness programmes.

The Trust should improve the DPOs day to day visibility over breach information and ensure it creates an Information Governance Risk Register where the various types of breach risk can be analysed and assessed.

The Trust should ensure that senior staff undertake specialised data breach training and that general staff training includes the three breach types and not just confidentiality.

Business continuity:

The Trust should ensure that any missing disaster recovery procedures are written up and ensure that manual fall-back procedures are in place that mirror electronic workflows.

The Trust should ensure that testing of disaster recovery plans includes cross-functional exercises, so that it can be sure that (non-) clinical operations and IM&T can work together seamlessly.

The Trust should ensure that it has detailed business continuity / disaster recovery plans in place with third parties. These should be periodically tested / audited to give positive assurance that the plans are functioning as described.

Where the Trust has critical remote systems / ongoing service provisions with third parties, it should ensure that any reporting back to the Trust serves to give adequate assurance on business continuity matters.

In addition to Cyber Security and possible sanctions that could be imposed by the CQC, the Trust should reflect the wider risk of non-compliance with GDPR and potential ICO sanctions in its corporate risk register.

Good Practice

Change Management

The Trust have an effective IT change management fully embedded procedure in place. It covers all access management, acting as a catch all for all departments, all employees, all individuals who require access to the computer network and all IT systems or applications managed by IT services. It will process standard requests such as joiners, movers and leavers access where approved protocols are in place as well as normal and emergency changes, where an approval process and authorisation has to be achieved. Senior management sign off at the appropriate level and no change is implemented without prior approval from operations. This is all achieved through a detailed policy, weekly change meetings, when the Change Advisory Board meets (emergency changes are escalated to the ECAB) and is subject to a robust review processes.

App Approval

The Trust's Use and Development of Apps Procedure ensure that all Apps defined as having a medical purpose, used within the Trust, have gone through a rigorous approval process. Requirements are identified and agreed prior to design, development or implementation of a new process or system ensuring that data privacy is at the centre of the decision making process. Full collaboration between the Device Safety Officer, the Clinical Safety Officer and the Information Governance Lead ensure a full risk assessment and DPIA is carried out. The App must comply with the Health and Social Act 2012 standards as well as GDPR before progressing to the next stage of approval. The App then has to go through a full implementation process and receive senior management sign off before being used.

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