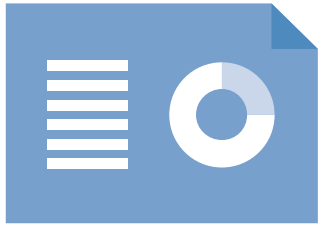
Brighton and Sussex University Hospitals NHS Trust

Data protection audit report

May 2018

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit. The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

The purpose of the audit is to provide the Information Commissioner and Brighton and Sussex University Hospitals NHS Trust (BSUH) with an independent assurance of the extent to which BSUH within the scope of this agreed audit, is complying with the DPA. In addition, where applicable, recommendations have been made to support compliance to the upcoming data protection legislation, namely the General Data Protection Regulations (GDPR).

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.

Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.
Requests for Personal Data	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.

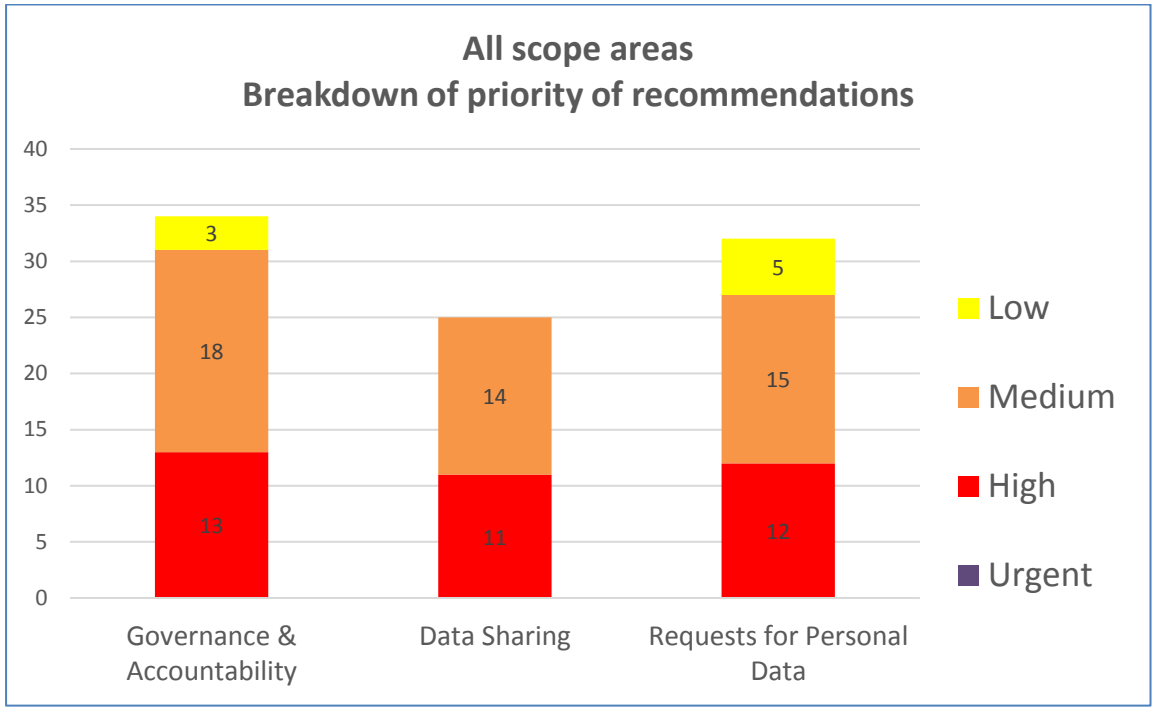
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA (but also in consideration of the pending GDPR). In order to assist BSUH 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. BSUH's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

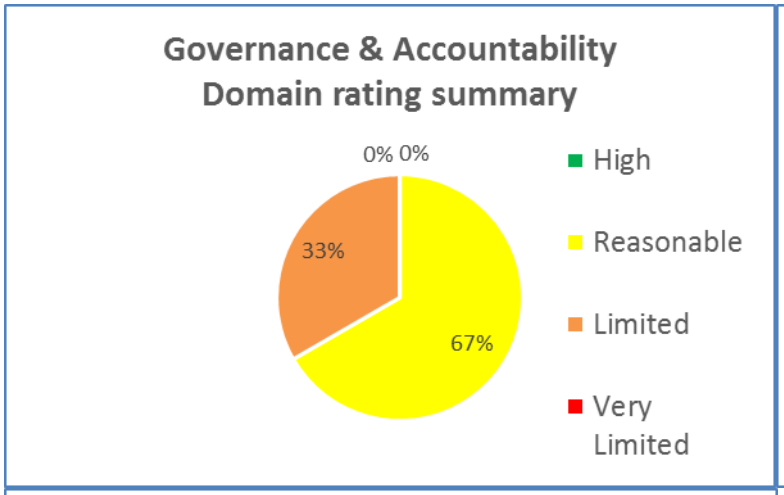
Audit Summary

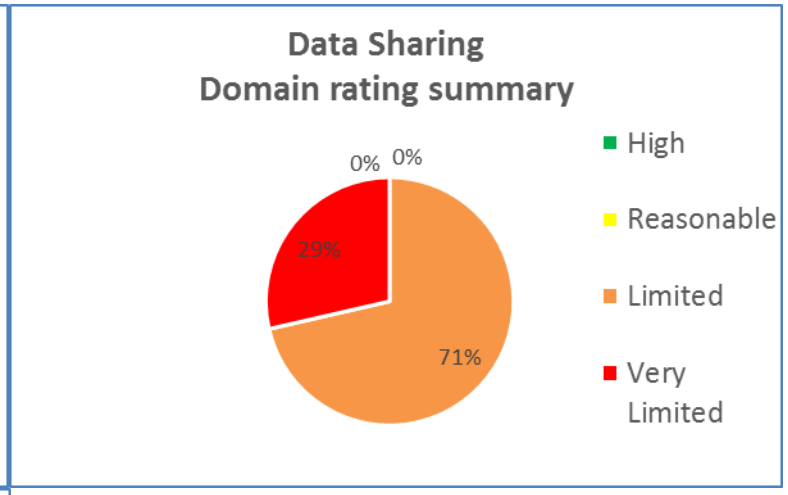
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce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

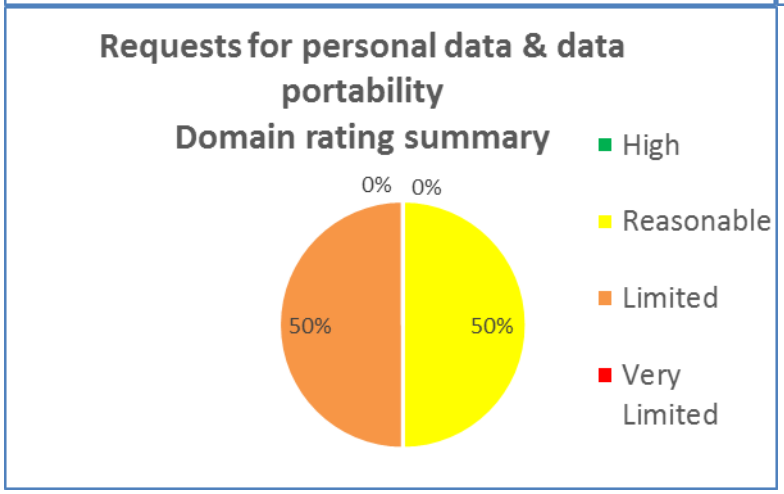
Priority Recommendations



Graphs and Charts







Areas for Improvement

BSUH is currently in a period of transition with a new joint Information Governance (IG) structure being created with Western Sussex Hospitals (WS) following a number of months of staff shortages due to sickness. While we note that there are plans in place to improve information governance at BSUH, the following are areas for improvement which we have identified during the audit.

Governance and Accountability:

A full governance structure which will allow BSUH to have oversight of IG activity and compliance should be implemented as soon as possible. BSUH should also review and reformulate their IG policies to provide a framework for the implementation of the overarching IG agenda within the new structure.

Contracts with Data Processors should include data protection clauses to provide assurance that data security arrangements are effective and comply with contractual agreements.

A system by which IG Key Performance Indicators (KPIs) are reported and reviewed regularly at senior management and Board Level should be put in place to provide oversight of the BSUH's IG compliance. This has particular importance as new data protection legislation comes into force.

Data Sharing:

All Information Sharing Agreements (ISAs) should include common retention and disposal periods. Where practical, specific retention policies should be implemented for the type of data being shared.

Ensure that appropriate security measures are in place and detailed in a formalised procedure taking into account the confidentiality of the data as well as any protective marking schemes that apply. Formalised guidance should be produced for staff in relation to recording and monitoring verbal and written requests on a data subject's file

and disclosures to 3rd parties.

Ensure that there is inbuilt oversight and approval / checking mechanisms in place prior to disclosures. Approved decisions should be regularly reviewed, scrutinised and recorded to ensure compliance and validity.

Requests for Personal Data:

Teams with responsibility for responding to subject access requests (SARs) are spread across a number of departments. There is no central oversight, joined-up communication or KPI reporting between teams. If this is to continue, BSUH needs to ensure that there are regular minuted meetings and cross departmental liaison to discuss the management of SARs received.

Ensure that staff members with responsibility to respond to SARs, across all departments, are sufficiently trained and receive specialised training where necessary in relation to the application of redactions and exemptions. This training should be reviewed and updated on a regular basis.

It should be clearly recorded when a redaction and exemption has been used, the reason why, and evidence provided of any advice sought. Ensure that a procedure is in place to approve SAR responses in order to ensure that data is redacted or withheld in line with regulations.

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 BSUH.

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