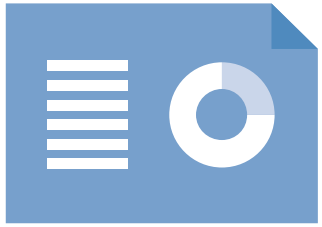
Betsi Cadwaladr University Health Board

Data protection audit report

July 2018

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the General Data Protection Regulations (GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision 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 purpose of the audit is to provide the Information Commissioner and Betsi Cadwaladr University Health Board (BCUHB) with an independent assurance of the extent to which BCUHB 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.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
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.

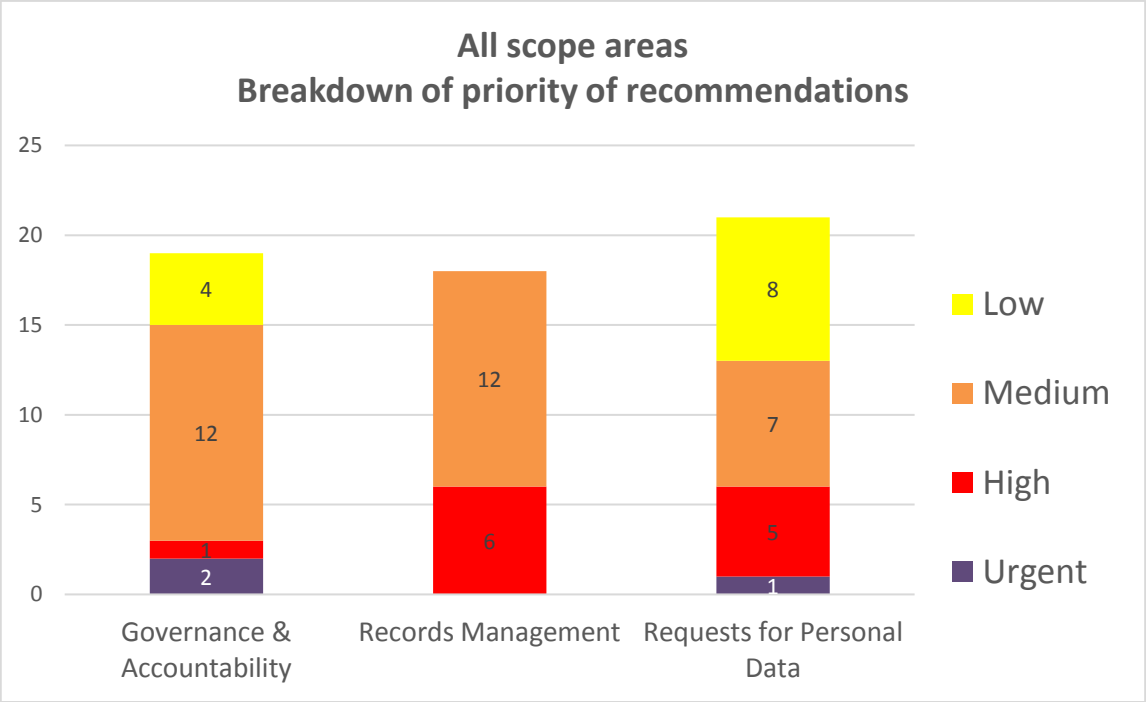
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist BCUHB in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. BCUHB's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

The ICO undertook a survey of BCUHB staff prior to the audit which received 955 responses. A summary of this survey can be seen at Appendix 2

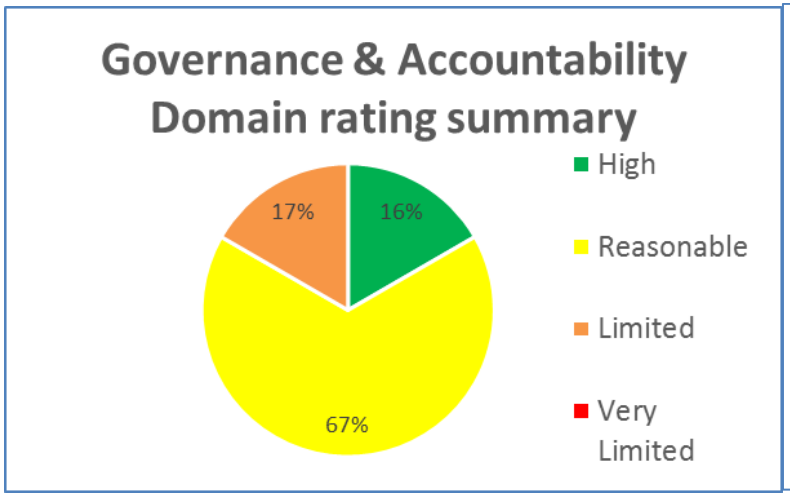
Audit Summary

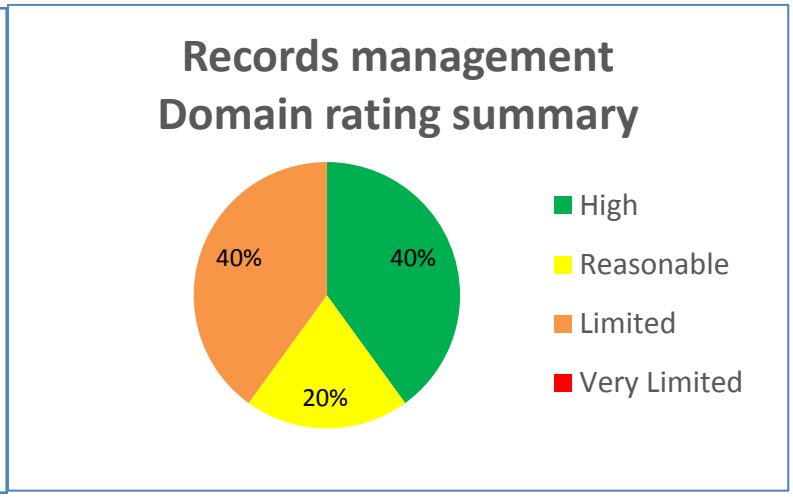
Audit Scope Area	Assurance Rating	Overall conclusion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to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

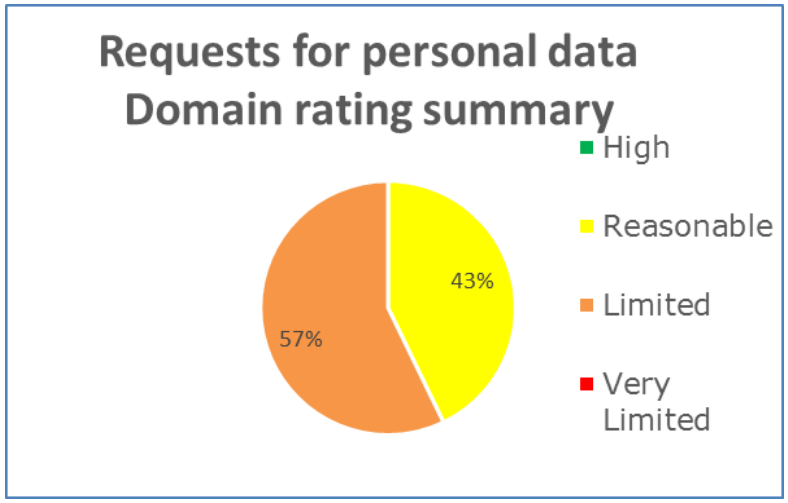
Priority Recommendations



Graphs and Charts







Areas for Improvement

Governance and Accountability:

Auditors identified a lack of fair processing information in a physical form. BCUHB should provide the public with information about how their personal data is being used. This information should be readily accessible and understandable, including to individuals who do not have access to BCUHB's website. Staff should be able to support individuals in finding out how their personal information is used.

BCUHB should ensure that both the information flow mapping exercise and the recording of all processing activities undertaken are completed in a timely manner.

BCUHB should consider additional methods of raising staff awareness of their responsibilities toward data protection compliance given the requirements under the new data protection legislation, and taking into account those staff who are hard to reach through briefings and the intranet.

Records Management:

Health Records at BCUHB fall under a number of different custodians. In order to ensure strategic direction and oversight for these records, the establishment of an executive member with lead responsibility for the direction and oversight of records management should be expedited. Measures to improve attendance at the Patients' Records Group should also be explored to ensure strategic direction and support is provided for the custodians of all patient records.

There are potential improvements to the security of patient records which should be considered. These include ensuring that key codes to areas where records may be held are changed regularly, and the need to ensure that the 'Therapy Manager' system is rolled out to all appropriate sections of the therapy service areas in the planned timescale to avoid the need to take physical records off site.

Requests for Personal Data:

Policies and procedures for handling subjects access requests (SARs) should be further updated to reflect changes brought in by the new legislation, such as the management of verbal requests. BCUHB should provide guidance to all staff to ensure that they are able to recognise and respond to verbal requests for personal data, so that they are channelled to an appropriate team. Priority should be given to the reception staff as the likely first point of contact.

Specialised training should be provided to all staff who are responsible for handling and processing SARs. This should include information about how exemptions are to be applied in line with legislation. There should be a Quality Assurance process undertaken for when information is being withheld under an exemption, involving at least one review of information being withheld prior to its disclosure. A standard method of redacting information should be introduced to ensure that redacted information cannot be revealed to the recipient.

A copy of the disclosure bundle showing the redactions or exemptions and the reasons behind them should be retained by BCUHB. This will mean that if a complaint about the quality of a SAR response is received, the organisation can understand whether the SAR was handled correctly or if further information should be released.

Good Practice

BCUHB has developed an exceptional Informatics Portal which provides the functionality for information flow mapping and an information asset register. As information owners or administrators enter details of information assets or systems, links are provided to appropriate policies and procedures, and risks can be identified. Reminders are sent a month before the retention date of information assets to alert owners or administrators to the fact they there are assets which need to be reviewed and possibly destroyed. Entries made on the system are reviewed and users are supported by staff from Information Governance.

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 BCUHB.

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