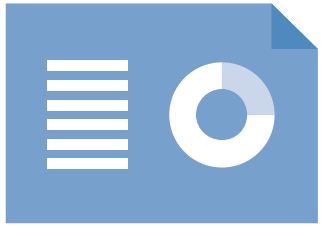
Optima Health

Data protection audit report

August 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.

Optima Health (Optima) approached the ICO requesting advice. On review of their application it was decided that due to the size of the organisation and their scale of data processing activities that they would benefit from an audit. Optima agreed to this approach and consented to an audit.

The purpose of the audit is to provide the Information Commissioner and Optima with an independent assurance of the extent to which Optima, 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
Requests for personal data, disclosures & lawful bases for processing	The extent to which Optima has procedures in place to recognise and respond to requests for personal data. This will include controls to ensure that individuals are given guidance on how to make requests, that staff are appropriately trained to recognise and process requests, that requests are dealt with within legislative timescales and that redactions and exemptions are appropriately applied. The procedures Optima has in place to respond to ad hoc third party requests for personal data including records of responses, validation and identification checks and approval or quality assurance checks against legislative requirements. The extent to which Optima has reviewed the various types of processing carried out and that the lawful bases or processing have been documented internally and are communicated to data subjects in the organisation's privacy information.

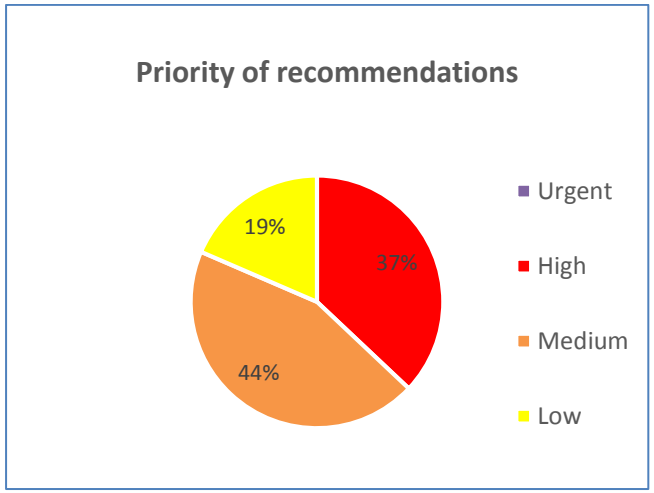
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Optima 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. Optima's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

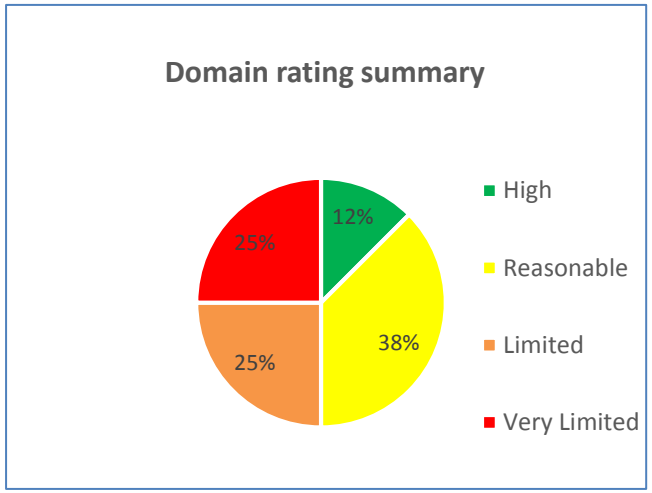
Audit Summary

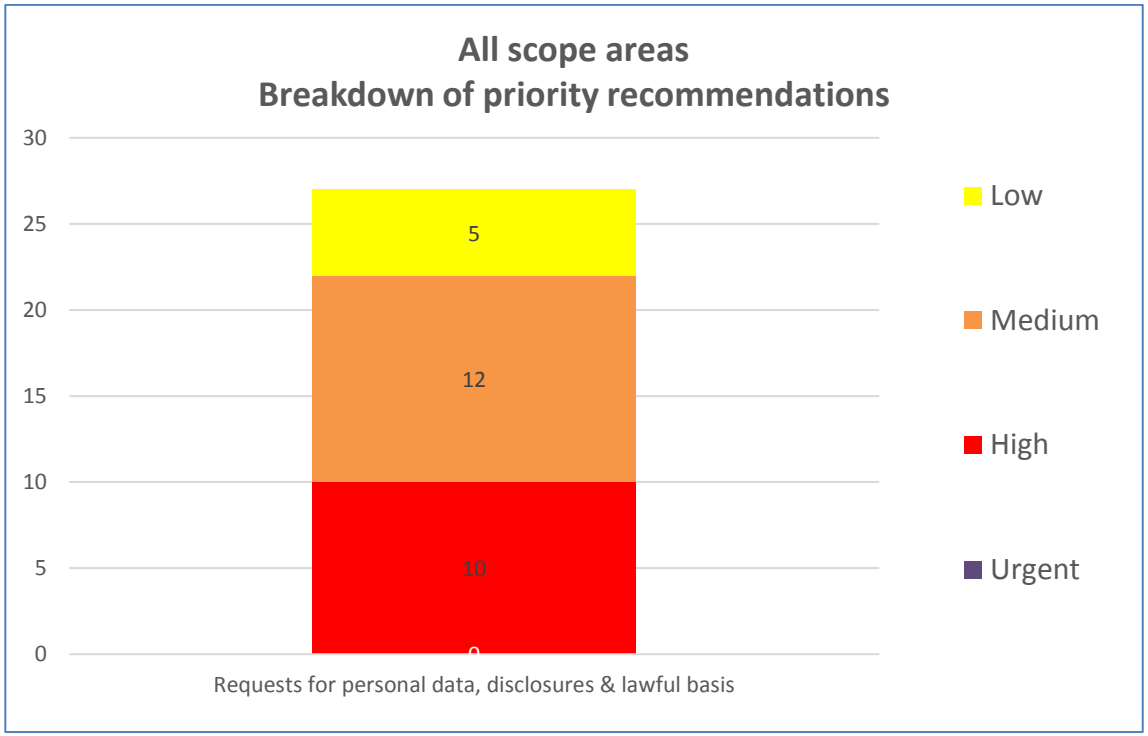
Audit Scope Area	Assurance Rating	Overall opinion
Requests for personal data, disclosures & lawful basis	REASONABLE	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations



Graphs and Charts





Areas for Improvement

Subject Access Requests:

The ICO's auditors observed experience and knowledge in staff responsible for administering requests, however in order to support GDPR compliance they will need to put in place a documented training programme and corresponding procedures to address specific areas of the role such as exemptions and redaction. These should be refreshed annually and the sessions and attendees recorded in the training logs. Optima should also train all staff to respond to verbal requests for personal information and update its procedures to ensure there is a method to allow individuals to make such requests by phone or in person.

Optima need to add further detail and relevant contact information to the SAR section of their privacy notice in order to make it clear what information individuals can ask for, when it will be received, the formats information may be sent in and any identification that may be required. Optima should also outline when a request may be partially or fully withheld or redacted.

Optima should ensure that there are written procedures in place for staff to follow on how to retrieve paper based and electronically archived data to provide a response within the legislative timeframe. This will ensure that no vital information is being missed as part of the SAR response.

Optima should ensure that any information that has been redacted or withheld completely is approved or independently checked to ensure the correct actions have been taken before it is disclosed to avoid inappropriate disclosures or too much information being withheld. The approval should be recorded for audit purposes.

Optima should include a paragraph in their covering letters where requests are refused, informing individuals of their right to appeal / complain to the ICO in order to meet the requirements of the GDPR.

Disclosures:

Although Optima has robust policies and training in place to handle ad hoc third-party requests for personal data, there isn't currently a formal process for a senior member of staff to validate and approve a disclosure request from a third-party before the disclosure is made. Optima need to develop a procedure to ensure that any ad hoc requests for personal data falling outside the MIC process are validated by a senior staff member and that the approval is documented.

Lawful Bases for Processing:

Optima needs to complete its information flow mapping exercise in detail and ensure that it fully completes its Record of Processing Activities (ROPA).

Optima has documented its lawful bases however there is some inconsistency across the documentation. Optima will need to ensure that their bases for processing different categories of information for various purposes are consistently documented to make sure they are effectively communicated in their privacy information.