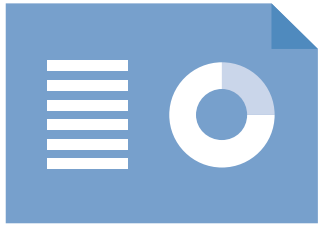
East London NHS Foundation Trust

Data protection audit report

June 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 purpose of the audit is to provide the Information Commissioner and East London NHS Foundation Trust (the 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**
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 their personal data.

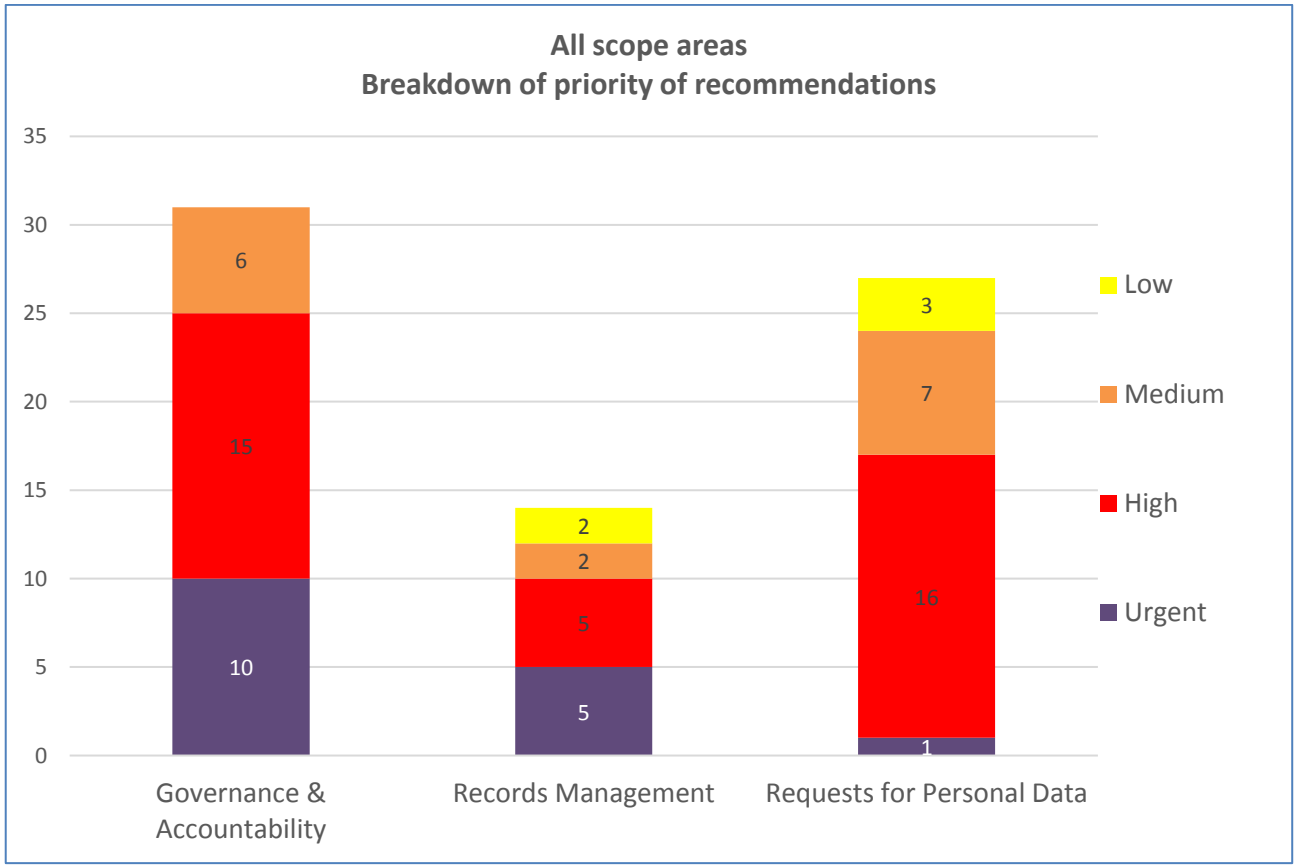
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

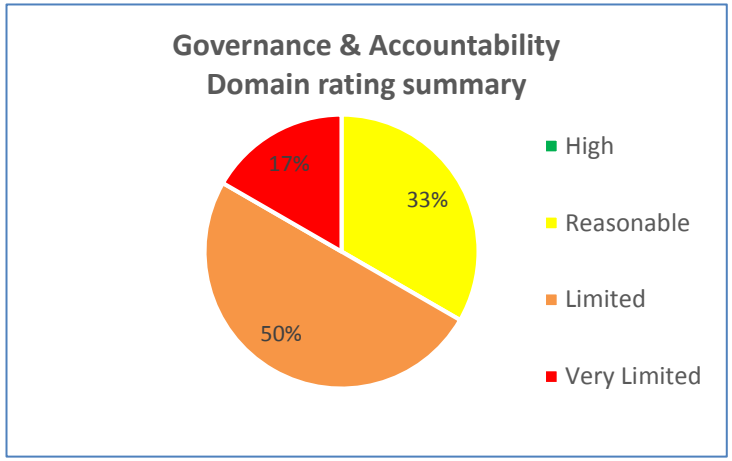
Audit Summary

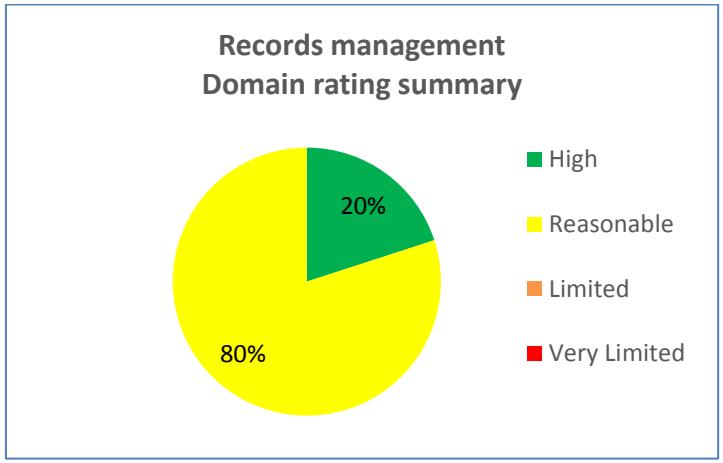
Audit Scope Area	Assurance Rating	Overall conclusion
Governance & Accountability	LIMITED	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements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

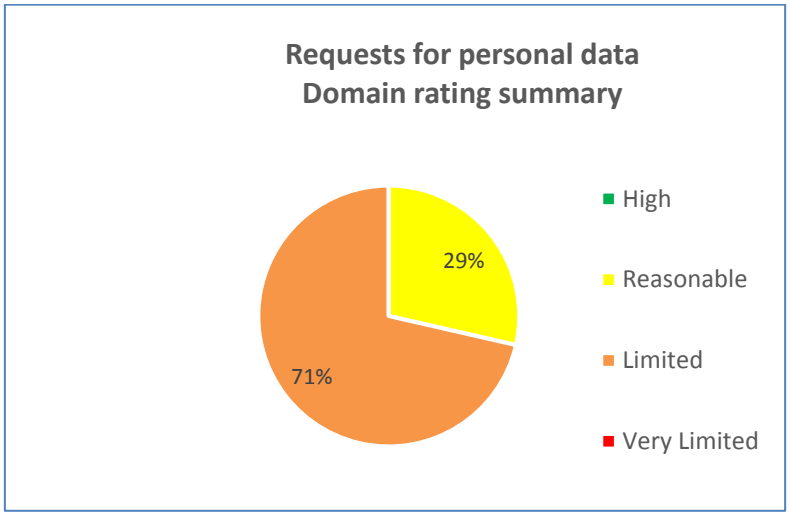
Priority Recommendations



Graphs and Chart







Areas for Improvement

Governance and Accountability:

Auditors identified a lack of clarity in the DPO job description. The Trust should ensure that the role and responsibilities of the DPO is clearly outlined in a job description in line with GDPR requirements. The Trust should also take steps to ensure that the DPO role has the appropriate level of independence and that this is supported and recorded in relevant policies.

The Trust needs to complete its contract review exercise to ensure that all written contracts with processors include the compulsory terms and details as outlined in the GDPR. It must also ensure that contracts include the technical and organisational measures processors will adopt as well as the obligations in relation to the notification of personal data breaches, complying with the rights of individuals and Data Protection Impact Assessments (DPIAs).

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

Records Management:

Although each area of the Trust has completed a local Information Asset Register (IAR), the Trust needs to continue its work on the overarching IAR and identify the lawful basis for processing for each asset.

The Trust has developed detailed internal training for its Information Asset Owners (IAOs) and Information Asset Administrators (IAAs), however it needs to ensure that all IAOs and IAAs complete the training in a timely manner to help them carry out their responsibilities effectively.

The Trust also needs to develop its policy and procedures in relation to requests for erasure as well as including a third party notification step as part of its requests for rectification of inaccurate data procedure.

Requests for Personal Data:

The Trust should develop processes to facilitate oversight of the SAR process by the IG team. This should include the IG department reviewing and approving SAR procedures that are issued to directorates. Furthermore, the Trust should audit existing processes across directorates and ensure that a consistent approach is taken.

The Trust should establish formal root cause analysis reporting into the IGSG for all breaches so that appropriate remedial action can be identified and acted upon.

The Trust should also develop standardised letters for requesters that explains the searches that have been made to deal with the request and where appropriate, explain if an exemption is used.