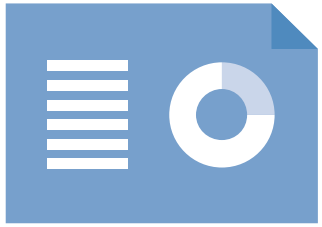
East of England Ambulance Service NHS Trust

Data protection audit report - Executive Summary

April 2019

ico.
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 of England Ambulance Service NHS Trust (the Trust) with an independent assurance of the extent to the Trust within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on several key areas of data protection compliance which included aspects relating to management structure, policies and procedures, information governance training, rights of access and transfer of records.

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.

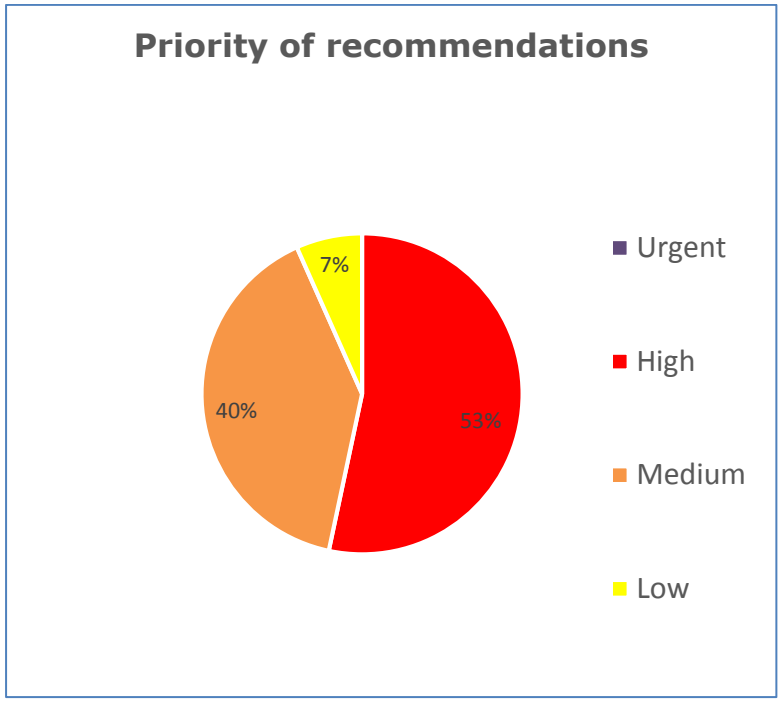
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that 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.

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

Assurance Rating	Opinion
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.

Graphs and Charts



Areas for Improvement

The Data Protection Officer (DPO) at the Trust is also the Information Governance (IG) Manager. This raises the risk of a conflict of interest between the roles and also of insufficient capacity and resilience within the role. The post of IG Manager should be separate to that of DPO. Furthermore, the operational independence of the DPO and their reporting link to senior management should be written into the appropriate IG policies.

The Trust should consider implementing a formal sign off procedure to gain assurance that staff have read and understood new and revised policies relating to information governance.

IG induction should be provided in a timely manner to new employees who will be handling personal data to reduce the risks of data protection breaches.

The Trust should continue with measures to improve the completion of mandatory training, and should also ensure that accurate figures for completion are being reported. All staff, including temporary and contract or agency staff should complete the training.

The time taken to respond to subject access requests (SARs) should continue to be monitored by the Trust, and resources applied appropriately to deal with the quantity of requests received to ensure that legislation is complied with.

In order to reduce the risk of unauthorised access to personal data, the Trust should put procedures into place to ensure that accurate details of staff roles and access requirements reach IT swiftly so that correct access permissions are in place.

Contracts held with any third party suppliers which transfer information should be reviewed to ensure that detailed security requirements are in place which comply with current legislation.

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