

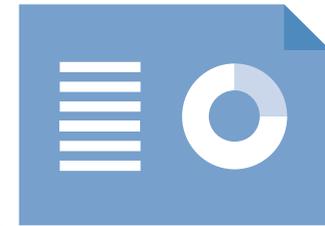
# South East Coast Ambulance Service NHS Foundation Trust

## Data protection audit report

June 2019

# 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 South East Coast Ambulance Service NHS Foundation 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.

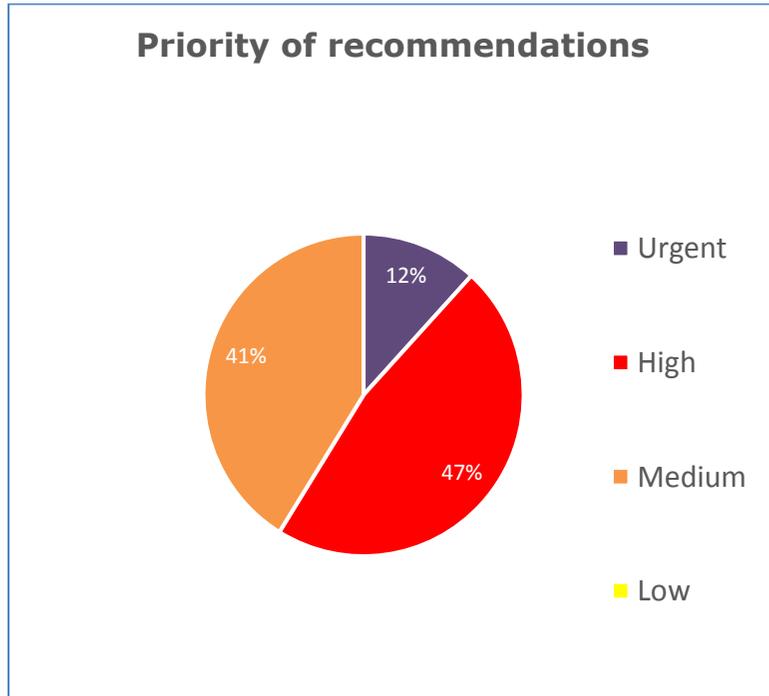
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that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

## 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.

## Priority Recommendations



## Areas for Improvement

### Management Structures:

- The Trust should ensure availability of appropriate personnel in the event of a serious data breach outside corporate hours so that it is assessed, escalated and if necessary reported to the ICO within the 72 hour timeframe.

### Policies and Procedures:

- Further assurance is needed that employees are keeping up to date and reading key policies. The Trust should consider introducing a formal sign off process to provide supporting evidence.

### Information Governance Training:

- The Information Governance training provision should be formalised in a policy which clearly outlines the Trust's approach to induction and mandatory training and details expected timeframes for completion.

### Right of Access:

- The Trust should ensure its guidance given to individuals on how to make a subject access request (SAR) is consistent and accurate. It also needs to ensure that all SARs being processed are logged to the same standard and monitored appropriately. More generally, sharing resources and standardising procedure within the three departments handling SARs, could improve response times.

### Transfer of Records:

- In order to reduce the risk of unauthorised access to personal data, controls around USB ports and removable media need to be tightened and compliance to policy monitored.
- The Trust needs to carry out an inspection of the 3<sup>rd</sup> party storage facility it uses as soon as possible and review the contract in place to ensure it is compliant with changes to Data Protection legislation.

## Good Practice

- The collaboration between the IG Team and the Quality Improvement Hub demonstrates good practice. IG issues are brought to the hub and practical solutions are sought to how best make improvements or changes at operational level. In turn, operational staff can feedback through the Hub if policies and procedures are not working effectively. This "sandbox" approach has been very successful in finding solutions to issues like making privacy policies accessible to paramedics to ensuring mandatory training delivery is effective. The IG team are now also dovetailing their audit visits to the Quality Assurance visits carried out by the Hub, helping to raise IG awareness and sharing the message that IG and quality assurance go together.
- The annual peer-to-peer review of the Trust's IG training by an independent Hospital Trust demonstrates that they are going to extra efforts to seek assurances that their IG training is at the appropriate standard.