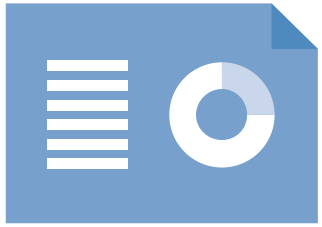
Southport and Ormskirk Hospital NHS Trust

Data protection audit report

September 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.

Southport and Ormskirk Hospital NHS Trust (The Trust) asked the ICO to conduct an audit of the Maternity department of the Women's and Children's CBU following a number of data breaches.

The purpose of the audit is to provide the Information Commissioner and 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**
Training and Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.
Security of Personal Data	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

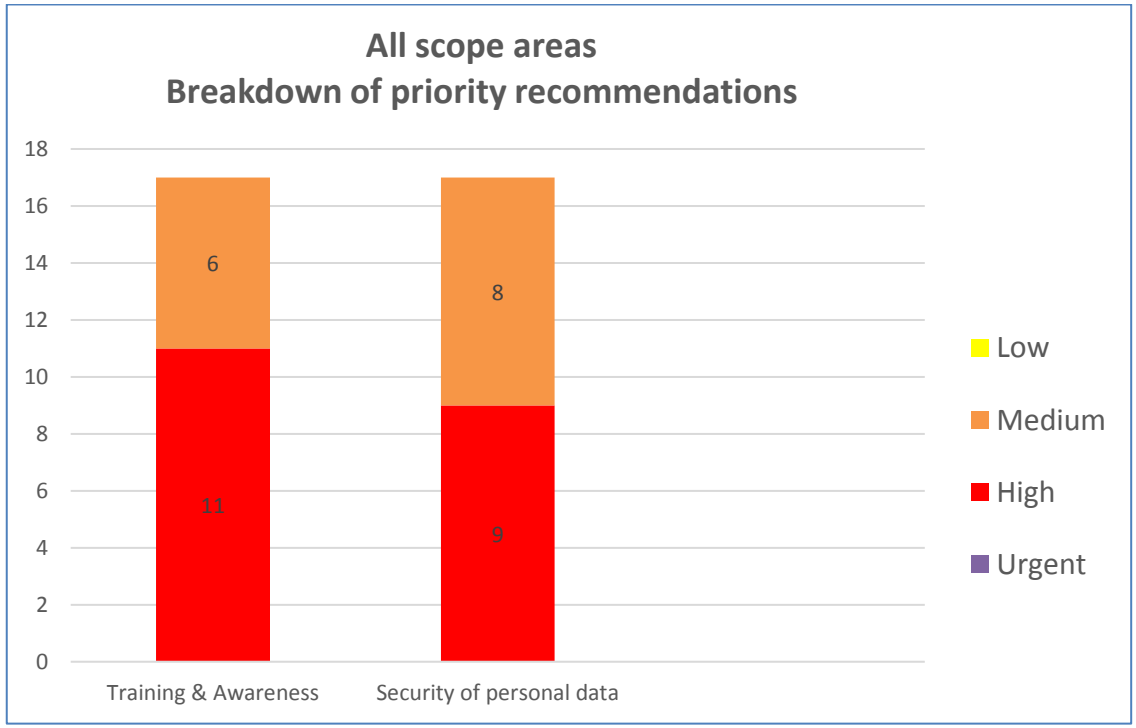
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records. The audit ratings and recommendations have been made on this basis, but the Trust may of course also wish to consider the recommendations in the context of the whole organisation.

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's 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.

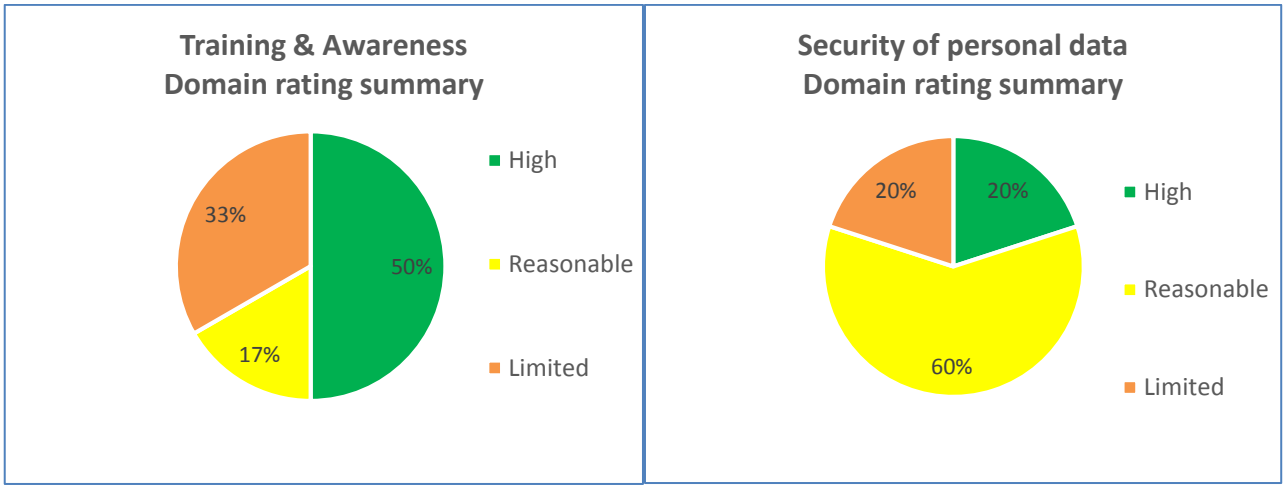
Audit Summary

Audit Scope Area	Assurance Rating	Overall opinion
Training & Awareness	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.
Security of personal data	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

Training and Awareness

The completion of the annual mandatory Information Governance (IG) training is below compliance levels throughout the Trust including in the Maternity Unit. The Trust should implement a strategy with appropriate resources and support to bring the completion levels up to compliance standards.

Bespoke training has been provided as a one-off event to address specific vulnerabilities, however, the Trust should conduct an analysis to identify where there are particular areas of vulnerability for data security and provide appropriate training on a regular basis.

IG training should be regularly reviewed to ensure it covers all legislation and meets the needs of the organisation. Once reviewed, it should be signed off by senior management.

Security of personal data.

The Trust has put actions in place as a result of previous data breaches to mitigate the risk of further breaches. These should be reinforced by a programme of spot checks and audits to ensure that staff are adhering to the IG policy and that issues are fed back appropriately.

The new IG Policy Handbook should be completed, ratified and disseminated to staff so that they can be aware of the most up to date guidance regarding information security, including the processes for escalating and responding to data security incidents.

The current review of policies should include robust procedures for the review and timely update of policies. As the IG structure is currently under review in the Trust, the Trust should make sure that any policies accurately reflect the responsibilities in relation to operational responsibility for the development and implementation of information security at the Trust and are disseminated appropriately to staff.

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