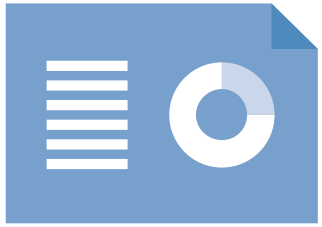
Sussex Partnership NHS Foundation Trust

Data protection audit report

March 2020

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 audit was conducted on a consensual basis and was part of a range of audits looking at the measures in place to maintain the security of personal data.

The purpose of the audit is to provide the Information Commissioner and Sussex Partnership 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:

Scope Area	**Description**
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

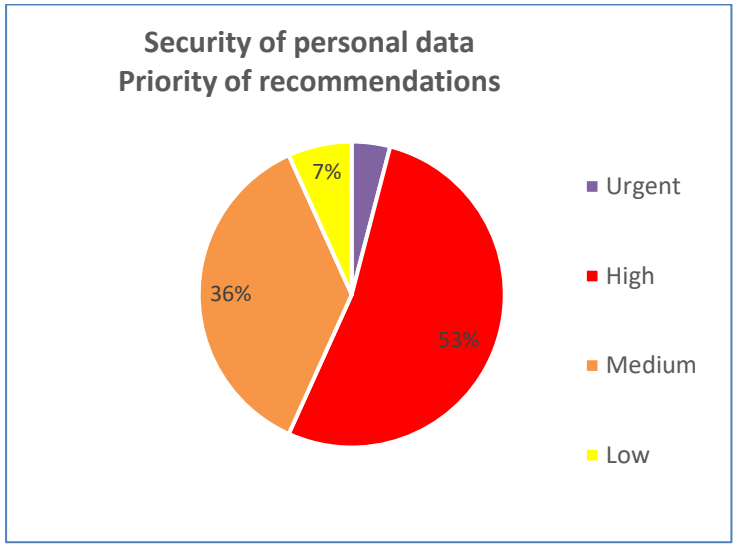
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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 Opinion
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



Areas for Improvement

The Trust's approach to Bring Your Own Device (BYOD) needs clarifying in policy as well as in practice. This is because BYOD is not explicitly prohibited in any policies whereas from interviews it is clear that the use of their own devices is discouraged.

The Trust does not currently have a process for retrieving hardware from former employees. It should develop a process that will ensure devices are returned upon termination of contract.

The Trust has not defined the measures it has in place to protect secure areas against environmental threats such as fire and flooding. This is important in areas such as the records store as there is a danger of paper records being destroyed.

The Trust does not have adequate oversight of its Data Protection Impact Assessments (DPIAs) or where there are gaps that need addressing. It should develop a central register of DPIAs for all of its data processing, complete DPIAs where they are missing and obtain assurance that risks have been mitigated before granting suppliers access to systems.

The Trust also should ensure that DPIA processes are formally embedded across PMO, procurement and change management processes and that relevant staff are trained to recognise the need for one and how they should be completed.

The Trust should ensure that the IG function is represented or consulted as part of all emerging technology and medical devices discussion groups so that IG risks can be identified and addressed as early as possible.

The Trust should ensure that it has mechanisms to regularly monitor access to patient data on an ongoing basis and that staff are always up to date with their IG statutory mandatory training before being granted access to systems.

The Trust should also ensure that it has recorded the granting of access rights to secure areas such as the records store and make sure that these access rights are reviewed on a regular basis.

The Trust should ensure that the information governance Training Needs Assessment (TNA) reflects all relevant staff groups, that it is scheduled for regular review and that clinicians receive specific training on exemptions and redactions on induction at the Trust.

The Trust's Information Governance department practiced clear desks and screens but this has not been recorded in a policy and so there is no assurance that this is being adhered to Trust wide.

Best Practice

The Trust conducts regular in house ethical hacking programmes to help identify weak passwords. The results are used to improve the strength of passwords used by staff. From this information staff would be contacted and asked to use a strong password.

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.