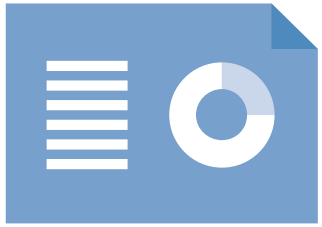
Isle of Wight NHS Trust

Data protection audit report

November 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.

In February 2018 the ICO undertook an audit of the Isle of Wight NHS Trust's (the Trust) processing activities in relation Records Management and Data Sharing. Following this audit the ICO provided the Trust with a full report which assessed that there was a very limited level of assurance that processes and procedures were in place and were delivering data protection compliance. The audit identified a substantial risk that the objective of data protection compliance would not be achieved. The report included 66 recommendations aimed at improving the Trust compliance with the legislation and reducing the risk of a data breach. The Trust accepted all b
ut one of these recommendations which was partially accepted. The Trust provided the ICO with details of the actions it intended to take to address the recommendations, an owner of these actions and a date by which they expected to have implemented the action.

The ICO contacted the Trust again in October 2018 in order to conduct a follow up engagement to assess the Trust's progress against the agreed actions. The Trust was asked to
provide evidence of the completion of recommendations or of work towards completion. This evidence was provided on 20 November 2018. The Trust was unable to provide evidence of any meaningful work towards completion for over half the

agreed actions and on this basis the ICO decided to conduct a full on-site audit in order to be able to gain an accurate picture of how the Trust's Data Sharing and Records Management provisions are performing now.

The purpose of this follow up 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 following the original audit of February 2018.

This engagement will revisit the scope areas covered in the original audit, these are:

Scope Area	**Description**
Data Sharing	The extent to which the design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation**.**
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.

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.

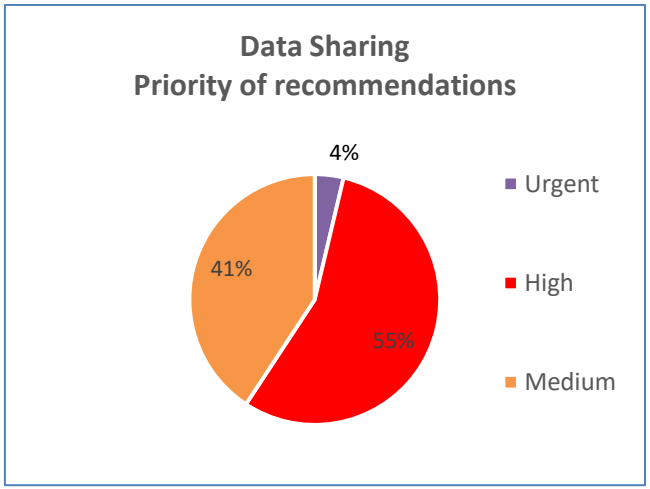
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that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

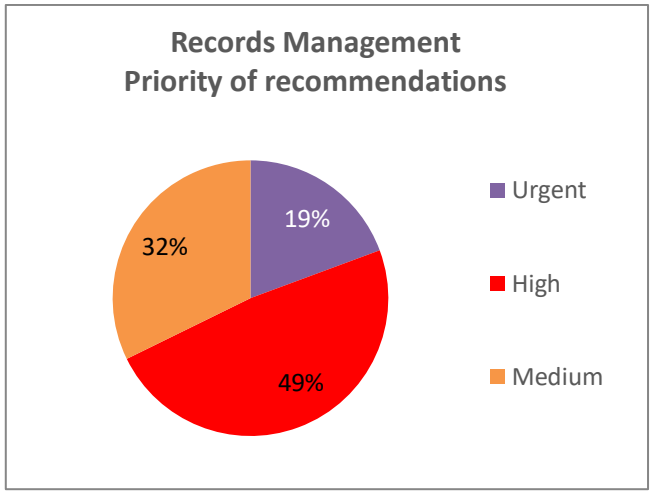
upon the ICO's assessment of the risks involved. The Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

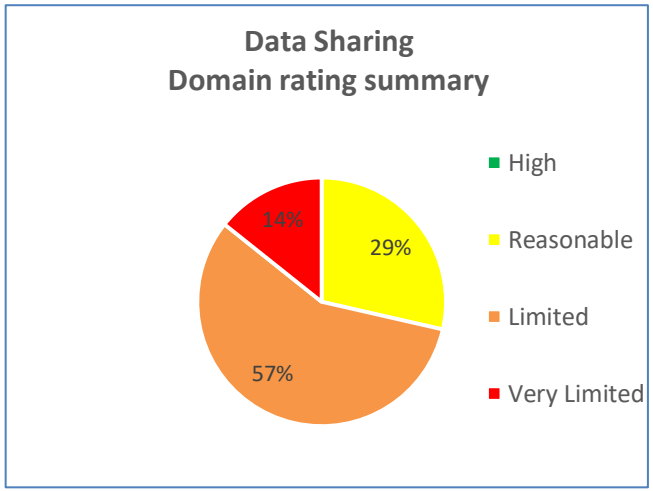
Audit Scope Area	Assurance Rating	Overall opinion
Data Sharing	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	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.

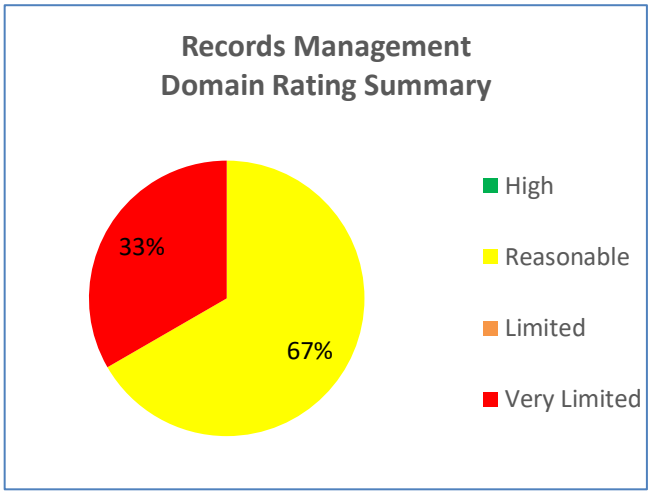
Priority Recommendations

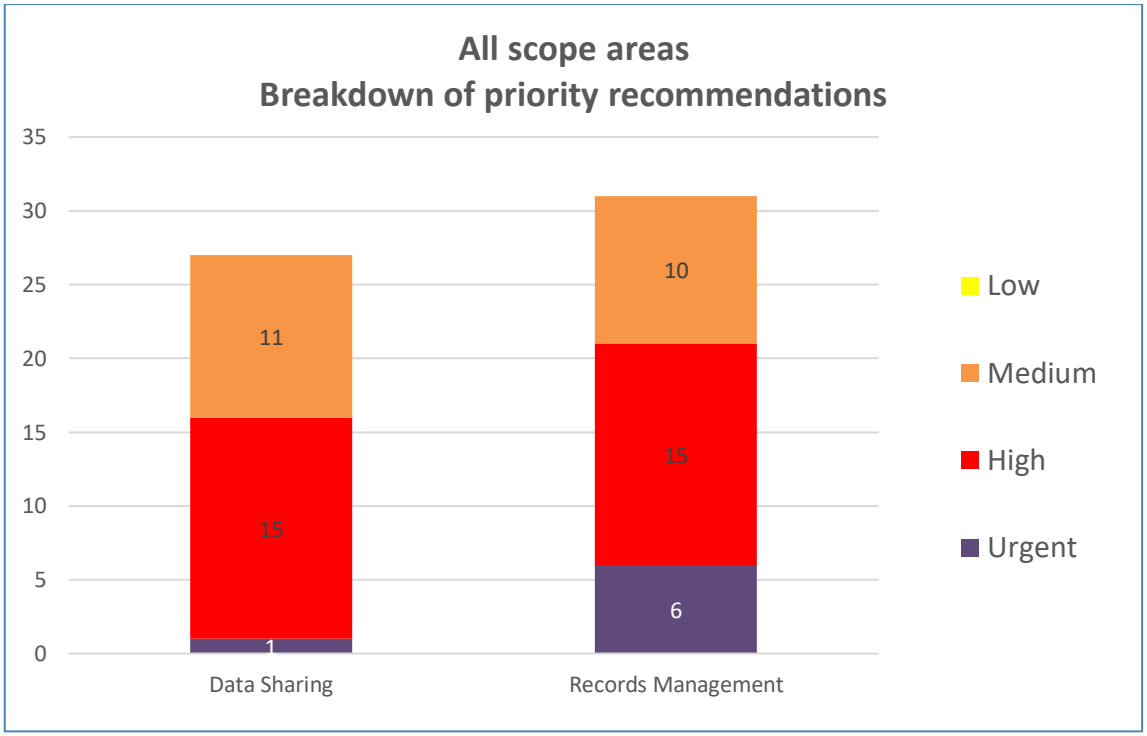




Graphs and Chart






All scope areas
Breakdown of priority recommendations
35
30
25
20
15
10
5
0
11
15
1
10
15
6
Data Sharing
Records Management
Low
Medium
High
Urgent

Areas for Improvement

Data Sharing:

Auditors identified a lack of oversight and tracking of data sharing agreements at the Trust. The Trust needs to formally identify all instances of regular or large scale data sharing with other data controllers and ensure that agreements are in place for these. Risks should be identified and mitigated as far as possible prior to signing up to agreements and they need to be reviewed regularly. Failure to identify and record all instances of regular or large scale data sharing with other data controllers puts the Trust at risk of breaching Article 5(2) of the GDPR.

The Trust should also ensure that data sharing agreements include start / finish dates and the applicable technical and organisational security measures required to ensure secure processing, as well as a clear division of responsibilities to manage the various elements of the agreements. Articles 32 and 5(1)(f), could be breached by the Trust's failure to ensure all data is shared securely

To ensure compliance with Article 35 of the GDPR the Trust should ensure that the Data Protection Impact Assessment (DPIA) process is fully defined and embedded across its change processes in line with GDPR requirements. The Trust should also be sure to perform its own Trust specific DPIA where it is part of a multi-partner sharing agreement.

The Trust needs to perform a training needs analysis in respect of data sharing practices and ensure that specialist additional training is provided for all relevant staff. Failure to ensure that staff are aware and capable of carrying out their duties puts the Trust at risk of breaching articles 32 and 5(1)(f).

The Trust needs to implement a formal logging procedure for ad-hoc disclosures so that their compliance with data protection can be monitored by the Information Governance (IG) function in order to comply with article 5(2), the accountability principle.

Records Management:

The Trust needs to re-instate the Information Asset Owner risk management structure or an equivalent control and reporting framework as soon as possible as this underpins most of its IG policies. This should be accompanied by specialised training for those given IAO / IAA responsibility. Failure to do so is likely to breach article 32 and 5(1)(f).

To ensure compliance with the accountability principle outlines in article 5(2) of the GDPR the Trust should ensure that departments create and review standard operating procedures as mandated by its overarching policies. These should be specific to each department's requirements but should be in line with the Trust's broader Records Management strategy, ensuring consistent approaches in tracking mechanisms, procedures in locating missing files and uniform retention periods.

The Trust needs to implement a targeted programme of records culling and report the results to the IGSC. This should create a centralised oversight of the approach taken, enable decision making based on realistic expectations and the allocation of resources to reduce records in line with the NHS code of practice plus full oversight of decisions about data retention. This will protect against breaching article 5(1)(e)

The Trust will also need to prioritise assessments into how it manages its electronic records as currently deletion and minimisation of its digital records is not taking place, and there is uncertainty over whether electronic records can be deleted on many of the Trust's systems. This will also demonstrate compliance with article 5(1)(e).

The Trust needs to ensure that further fair processing information is provided to patients beyond the privacy notice on the website. CCTV signage must be put in place in areas where it is in operation to inform patients and staff. Failure to do so could put the Trust in breach of articles 5(1)(a), 12, and 13 of the GDPR

To ensure the Trust is not in breach of the previous articles of GDPR it should also update fair processing leaflets in use across the estate and consider additional methods to inform patients proactively as to how their data is collected, the purposes and legal bases for processing, how and with whom it is shared, and outlining the rights individuals have and how they can exercise them.

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