Isle of Wight NHS Trust

Data protection audit report

Executive Summary
March 2018

1. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

Isle of Wight NHS Trust, henceforth referred to as the Trust, agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 4 January 2018 with representatives of the Trust to identify and discuss the scope of the audit.

The audit field work was undertaken at St Mary's Hospital between 27 and 28 February 2018.

2. Scope of the audit

Following pre-audit discussions with the Trust, it was agreed that the audit would focus on the following areas:

a. Records management (manual and electronic) – The processes in place for managing both manual and electronic records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

b. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit Approach

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 purpose of the audit was 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 the DPA.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

In order to assist data controllers in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact	**Severe**	**High**	**High**	**Urgent**	**Urgent**
	High	**Medium**	**Medium**	**High**	**Urgent**
	Medium	**Low**	**Medium**	**Medium**	**High**
	Low	**Low**	**Low**	**Medium**	**High**
		Remote	**Unlikely**	**Likely**	**Very Likely**
		Likelihood			

It is important to note that the above 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.

4. Audit opinion

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 the DPA.

Overall Conclusion	
Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment. We have made 1 limited and 1 very limited assurance assessment where controls could be enhanced to address the issues.

5. Summary of Recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of the DPA.	We have made **2** urgent priority recommendations across both scope areas, Both of these are in the Records Management scope, where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **24** high priority recommendations across all both scope areas: **17** in Records Management; and **7** in Data Sharing, where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **33** medium priority recommendations across both scope areas: **20** in Records Management; and **13** in Data Sharing, where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **4** Low priority recommendations across both scope areas, all in the Records Management scope, where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

The Trust's Records Management (RM) Policy is well written and provides an overarching steer for Information Asset Owners (IAOs) in terms of their duties for RM. However, there is a lack of detailed procedural guidance for IAOs to follow.

The Information Governance (IG) department has copies and oversight of all Data Sharing Agreements (DSA) to which the Trust is a signatory.

Areas for improvement

The Trust does not have a Corporate Records Manager to provide Trust wide oversight of the RM function

Much of the responsibility for RM lies with the nominated IAOs. However, a large number of IAOs have failed to attend the forum set up to discuss IG issues (which has resulted in the disestablishment of the forum), and are not carrying out their IG responsibilities effectively.

There is no overarching Trust wide, up to date, Information Asset Register and no consistency in creating and applying retention schedules, with some data kept indefinitely.

The lack of fair processing information provided to patients is concerning as the Trust is likely to be breaching the first principle of the current DPA '98 by failing to provide information to patients about how their data is processed.

The Trust's DS framework document lists consent as the legal basis for sharing information. This currently unlikely to be the most appropriate basis for sharing data and will certainly need reviewing before the impending changes to data protection law.

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.