Heart of England NHS Foundation Trust

Data protection audit report

Executive summary
February 2017

Information Commissioner's Office

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.

Heart of England NHS Foundation Trust (the Trust) agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 28 September 2016 with representatives of the Trust to identify and discuss the scope of the audit and to agree the schedule of interviews.

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. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

3. 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.

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA. We have made 2 limited assurance assessments where controls could be enhanced to address the issues which are summarised below.

4. Summary of audit findings

Areas of good practice

Both the Information Governance (IG) Policy and the Data Protection and Confidentiality Policy have recently been reviewed, with a monitoring and review matrix added to each policy to monitor compliance. The monitoring success criteria for both the IG Policy and the Data Protection and Confidentiality Policy are the progress against the IG work programme, incident analysis, uptake of IG training and IG Toolkit Annual Assessment. Compliance against policies is also monitored via monthly reports submitted by the Policy Assurance Officer (PAO) to the Policy Review Group (PRG).

There is a comprehensive fair processing notice available on the Trust website. The "Fair Processing Notice for patients" covers why the Trust collects information, how records are kept confidential, other organisations the Trust may share information with (whether that be NHS or non-NHS), as well as contact details for the IG team at the Trust.

The IG team and the Communications team have worked together to create an IG Framework Awareness Plan to identify areas where the Trust's Communications Team can raise awareness of IG issues, policies, procedures and training.

Areas for improvement

The Trust acknowledges there is a gap in reporting at present, from the Information Governance Group (IGG) to the Trust Board. The IG Policy states the IGG should report up to the Chief Execs Group which in turn should report up to the Board, but no evidence has been provided of this happening in practice.

At present, there is no requirement for Information Asset Owners (IAOs) to provide assurance to the SIRO on an annual basis on the progress against monitoring and managing risks to their assets. Nor has evidence been provided of the SIRO's annual report to the Trust Board on Information Risk Management, as set out in the Information Risk Management Policy, which requires an annual report to set out the status of risks to information assets.

Results from the staff survey indicate a mixed level of awareness of the reporting procedure for cyber security incidents, with under half of respondents aware of the need to report an incident on Datix.

All Trust staff, including bank staff, attend a corporate induction on their first day at the Trust which covers their mandatory training, including IG training. The staff facilitating the induction training are not part of the IG team, and have no additional IG training above the mandatory requirements.

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 Heart of England NHS Foundation 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.