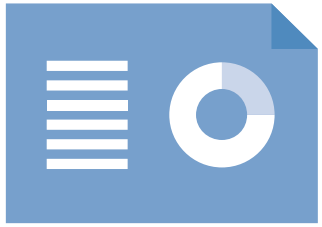
NHS England

Data protection audit report

January 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.

NHSE volunteered for a programme of audits by the ICO and these were formally agreed in September 2018. The audits are to be undertaken at agreed dates throughout 2018/19. For the first of these audits it was agreed the scope would focus on the following area:

Scope Area	**Description**
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.

The purpose of the audit is to provide the Information Commissioner and NHS England (NHSE) with an independent assurance of the extent to which NHSE, within the scope of this agreed audit, is complying with data protection legislation.

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.

NHS organisations across England were out of scope of the audit; the audit encompassed NHS England as a corporate entity only. Consequently the audit predominantly focussed on the processing of personal data within NHS England's internal corporate functions for which it is a data controller and is required to demonstrate compliance as an organisation in its own right.

The audit was conducted in two parts, the first being a central review of the overarching information governance (IG) framework, policies and procedures and organisational structures conducted at the Leeds Head Office. The second part consisted of a regional review of the application and compliance to the overarching policies and procedures and the regional frameworks in place to support data protection. The following regional IG Teams took part in the audit:

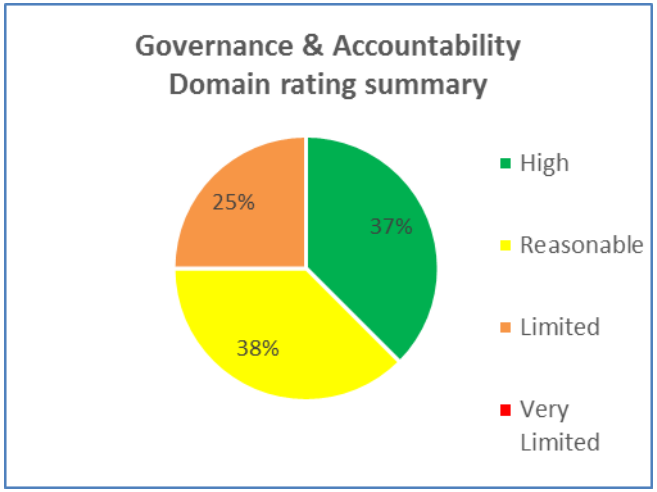
North Region
South Region
London Region
Midlands and East Region

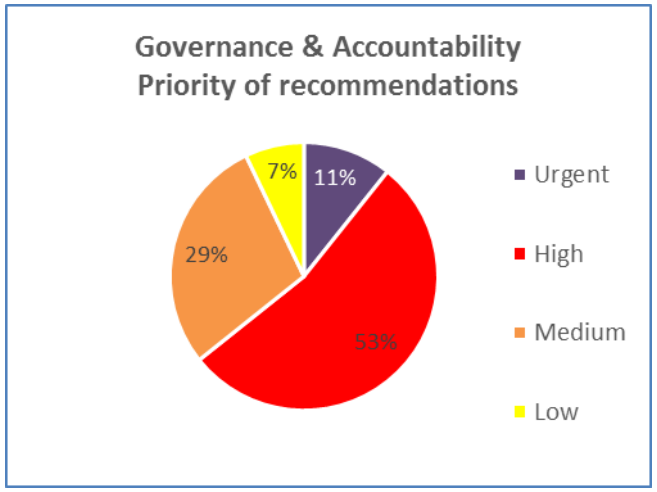
Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NHSE in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. NHSE'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
Governance & Accountability	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.

Graphs and Charts





Areas for Improvement

NHSE should continue with their work to ensure all existing data processor contracts have been updated to include the compulsory details and terms as outlined in the GDPR. In addition, NHSE should ensure that they put procedures in place to monitor a data processor's compliance with contractual requirements under GDPR on an ongoing periodic basis, paying particular focus to routine compliance checks to test processor staff data protection training completion, processor staff awareness and understanding of data protection policies and procedures, that data security arrangements are effective and comply with contractual agreements, that there are procedures in place for the notification of personal data breaches, and that there are procedures in place for complying with the rights of individuals e.g. requests for personal data.

An information flow mapping exercise has yet to be fully completed and verified for accuracy to confirm the various types of processing being carried out across NHSE and work is still ongoing to complete the IAM system to provide a central log of all information assets.

NHSE should revise the current Information Management Audit Framework to mandate more frequent audits of locality offices to provide assurances more widely of compliance to data protection legislation.

The information governance induction training is not consistently completed within a month of an employee's start date. NHSE should continue their work to identify or develop appropriate refresher training following operational changes this year which includes the key elements noted. The training should be mandatory and be completed on an annual basis.

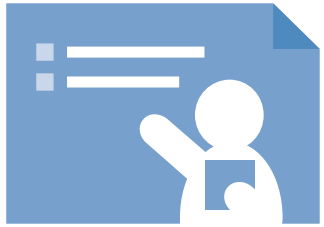
Good Practice

NHSE have developed a Contracts Management Toolkit which is due to be launched imminently across the organisation as a guide for all managers in the management of all contracts, from initial project initiation to implementation. The Toolkit will also contain contract templates, including data processor contracts, and checklists to assess suitability. The rollout will be supported by a training programme for all contract managers.

NHSE are in the process of establishing a new Assurance Function within the central IG Team, who will be responsible for managing and auditing compliance to data protection legislation across NHSE and by all data processors, assessing compliance with key IG policies by NHSE staff, providing consolidated reporting on IG related KPI and co-ordinating all national and regional IG related meetings and forums.

NHSE's overarching privacy notice contains a description of each of their main processing activities and the lawful basis for each of these is clearly noted. The notice is easily accessible via the website and is updated on a regular basis.

Appendices



Appendix One – Recommendation Priority Ratings Descriptions

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 data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

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 NHSE.

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