East of England Ambulance Service NHS Trust

Data protection audit report

October 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOI 2000) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

East of England Ambulance Service NHS Trust (the Trust) agreed to a consensual audit of its data protection and FOI practices.

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 data protection and FOI legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust's processing of personal data and FOI practices. The scope may take into account any data protection and FOI issues or risks which are specific to the Trust, identified from ICO intelligence or the Trust's own concerns, or any data protection and FOI issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of the Trust, the nature and extent of the Trust's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the Trust.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Governance and 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 UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.
Freedom of Information	The extent to which FOI/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.
Awareness	There are appropriate measures in place to raise and monitor awareness of data protection regulation requirements relating to staff's roles and responsibilities.

Audits are 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, remote interviews with selected staff, and a virtual review of evidential documentation.

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.

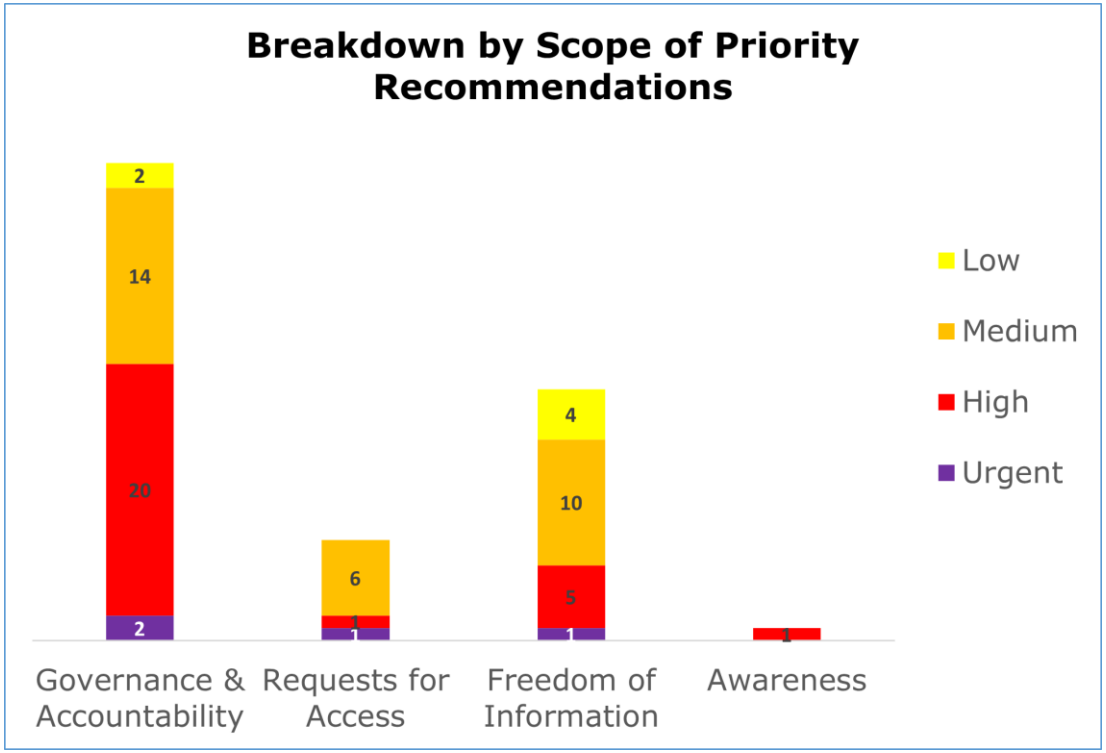
Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and 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.
Requests for Access	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.
Freedom of Information	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.
Awareness	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.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

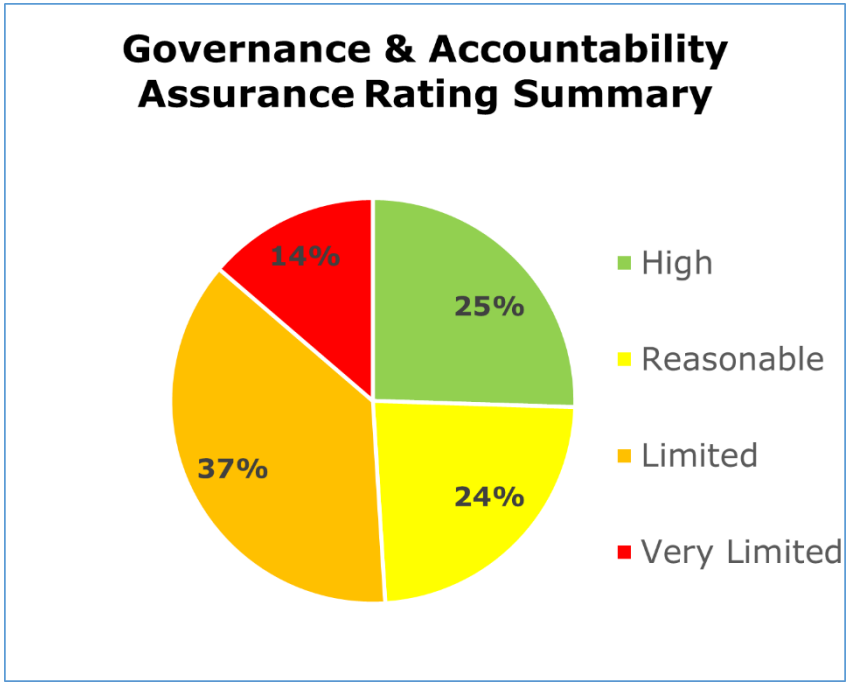
Priority Recommendations

The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

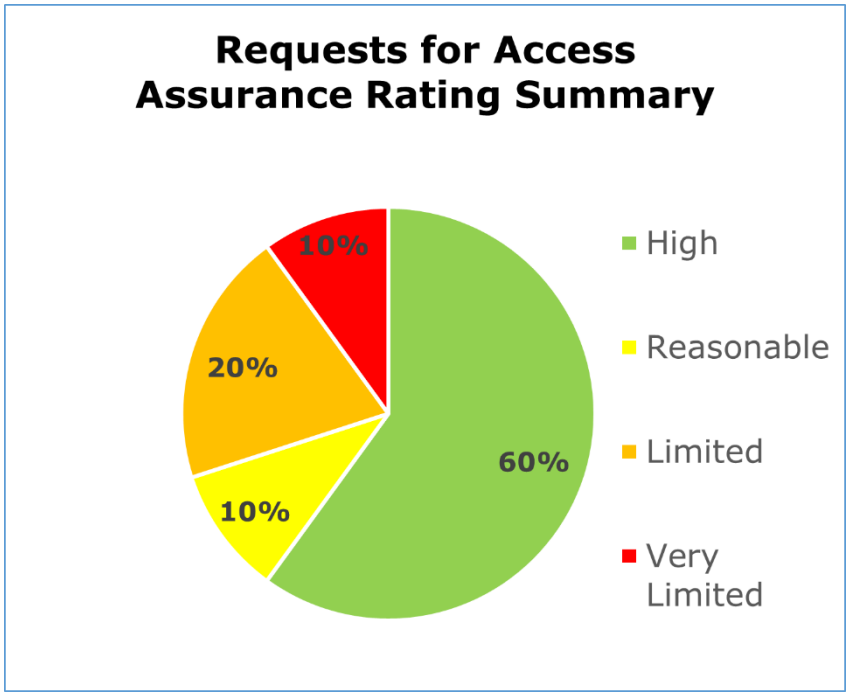


- Governance and Accountability has two urgent, 20 high, 14 medium and 2 low priority recommendations
- Requests for Access has one urgent, one high, six medium and no low priority recommendations
- Freedom of Information has one urgent, five high, 10 medium and four low priority recommendations
- Awareness has no urgent, one high, no medium and no low priority recommendations

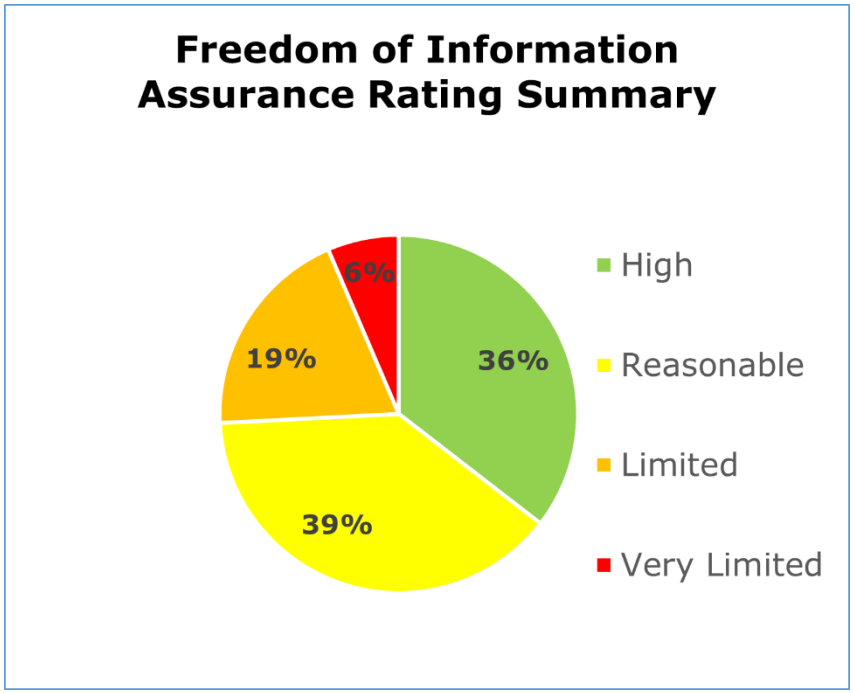
Graphs and Charts



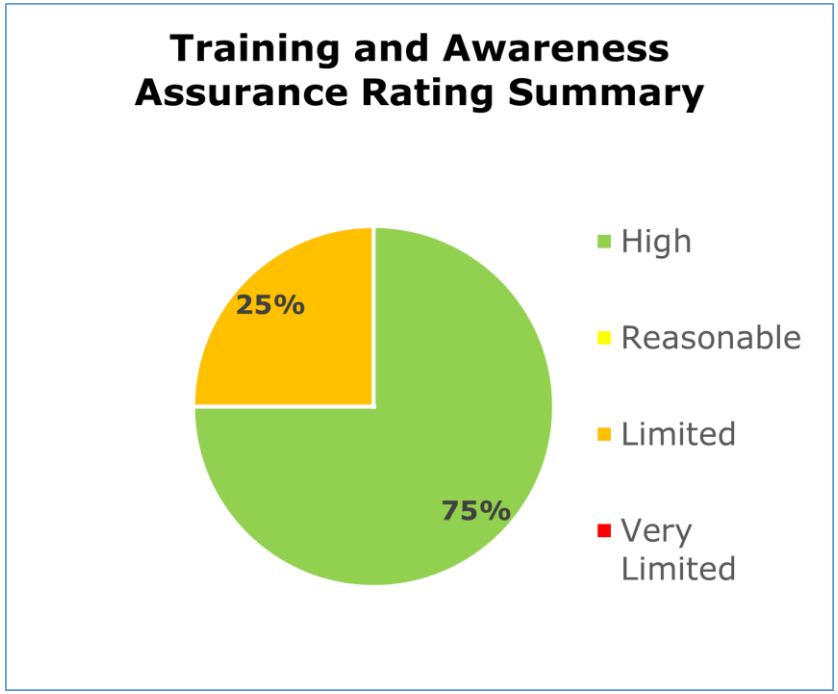
The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 25% high assurance, 24% reasonable assurance, 37% limited assurance, 14% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 60% high assurance, 10% reasonable assurance, 20% limited assurance, 10% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 36% high assurance, 39% reasonable assurance, 19% limited assurance, 6% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Awareness scope. 75% high assurance, 0% reasonable assurance, 25% limited assurance, 0% very limited assurance.

Key areas for improvement

We identified some key areas within our audit, where the Trust needed to implement further measures to comply with data protection law.

Governance and Accountability:

- The Trust must ensure it has identified and documented an appropriate UK GDPR article 6 lawful basis for all processing activities, as well as any additional conditions in the UK GDPR and DPA 2018 relevant to its processing of special category (SC) and criminal offence (CO) data. Where the Trust relies on article 6(1)(c) 'legal obligation' to process personal information, it must also document the relevant obligation under law in order to rely on this basis and include this within relevant privacy information.
- The Trust must ensure that it has an appropriate policy document in place to support its relevant processing of SC and CO data.
- The Trust must review and, where necessary, update its published privacy information to ensure that it meets the requirements of UK GDPR articles 13 and 14.
- The Trust should ensure that the DPO is performing their full range of duties in line with UK GDPR article 39, and that they are making full use of all available channels to regularly raise and address DP compliance issues with senior management at the Trust.

Requests for Access:

- The Trust must ensure that all Subject Access Requests (SAR) are processed and responded to within the statutory timeline. When this is not achieved the Trust is in breach of article 15 of UK GDPR.
- The Trust must ensure that it provides appropriately detailed guidance on the information released to the requester, including an explanation of what searches have been undertaken, and an overview of what

information has been provided as a result of those searches. If this is not explained properly, data subjects may not feel like their request has been answered or may misunderstand the answer.

- The Trust must ensure that the guidance to individuals on how to make a SAR includes explanation on how to make a verbal SAR. If data subjects are not given sufficient guidance, they may not be aware of their rights.
- The Trust must ensure that the guidance to individuals on how to make a SAR is available in a paper format. Without having the guidance available in a paper format, data subjects without access to the internet may not be fully informed of their right to request access to personal information.
- The Trust should have written procedures for all processes related to receiving, handling, managing and responding to SAR.

Freedom of Information:

- The Trust must ensure it meets statutory timescales for responding to FOI requests, as at the moment the Trust is not compliant.
- The Trust must ensure that all contracts allow access to, or provision of, applicable information within a suitable timeframe when requested by the Trust.
- The Trust must ensure that the staff responsible for handling FOI requests receive appropriate, specialist training with periodic refreshers. No specialist training for FOI staff has been provided since 2018.
- The Trust lacks written procedures in multiple areas, including identification and response to vexatious, manifestly unreasonable and repeat requests, and provision of the disclosure in a format preferred by the requestor.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

Governance and Accountability:

- The Trust has a programme of external audits in place to help provide independent assurance around the existence and effectiveness of its internal control environment.
- All policies and procedures seen by ICO auditors clearly set out how compliance with each will be monitored and there is evidence to show that governance bodies such as the Information Governance Group (IGG) have oversight of such monitoring.
- There are information governance and data protection key performance indicators (KPIs) in place, and performance to KPIs is reported and reviewed regularly by relevant stakeholders including the IGG to inform their subsequent decisions and actions.
- There is a formally documented data protection impact assessment (DPIA) process in place to help ensure that staff approach DPIAs in a consistent manner.
- There are strong and robust procedures and operational practices in place to ensure that personal data breaches are detected, reported and investigated effectively, and that the ICO and affected individuals are notified where required in a timely manner.

Requests for Access:

- There are clear governance structures to provide appropriate oversight of SAR processes and performance. Furthermore, they ensure appropriate escalation of SAR matters and figures.
- The CYCFreedom system used to manage SAR requires to log a high amount of information about the requests, which is then pulled from the system and used to monitor trends.

- The SAR team maintains close working relationships with teams which receive SARs, and which perform searches for information required for SAR disclosures. This is achieved through measures like monthly meetings where teams update on their progress and any outstanding requests.
- The CYCFreedom system automatically logs information on all actions like the name of the person who performed the action, date and time. This allows for a clear and robust audit trail.
- The SAR team marks all disclosed documents with a watermark of the SAR case reference number, name of the requester and date of the release. This ensures that all disclosed documents can be tracked back to the requester and the source of any further disclosures can be identified.

Freedom of Information:

- There is clear governance oversight in place to ensure compliance with FOI regulations, including IGG, regular reports to the Audit Committee with a yearly FOI Deep Dive Report.
- FOI team builds and maintains positive working relationships with teams which provide information for FOI disclosures. This also leads to good visibility of the FOI team across the Trust.
- Redactions are applied on a case-by-case basis and with an appropriate oversight.

Awareness:

- Awareness of IG matters is raised across the Trust using various media, including e-mails, MetaCompliance bite-sized videos, articles on the Trust's intranet and screen savers.

Best Practice

Governance and Accountability:

- The practice of sending six- and three-monthly reminders to policy owners ahead of a specific policy or procedure's Valid Until Date (VUD) is a strong, proactive measure to help ensure documents are reviewed in good time. Additionally, the reporting in detail of the overall policy compliance rate and identification of individual documents nearing and exceeding their VUD at IGG meetings provides good oversight and awareness to senior staff in this area.

Observations

The points below are observations made by auditors during the course of the audit to provide the Trust with advice to enhance compliance.

Governance and Accountability:

- The Trust could ensure that the date of last review is clearly shown in all published privacy information so that individuals are aware of when a review last took place.
- The Trust could include diagrams or illustrations within its DPIAs to clearly set out the relationships and data flows between controllers, processors, data subjects and systems.

Requests for Information:

- Auditors noted that the 'Consent Forms' which are sent to requesters as a way of asking for proof of ID and address may cause some confusion due to their name, as consent should not be the lawful basis for processing this information. The Trust could consider renaming these forms.
- The Trust could consider the application of an extension to the statutory timescales for response for complex requests on a case-by-case basis.

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