# Tees, Esk & Wear Valleys NHS Foundation Trust

## Data protection audit report

January 2022

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 (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 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.

The audit was conducted consensually as part of our ongoing audit strategy.

The purpose of the audit is to provide the Information Commissioner and Tees, Esk and Wear Valleys NHS Foundation Trust (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.

The scope areas covered by this audit were determined following a risk based analysis of the Trust processing of personal data. The scope may take into account any data protection issues or risks which are specific to the Trust, identified from ICO intelligence or the Trust own concerns, and/or any data protection issues or risks which affect their 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 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 & 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. |
| **Data Sharing** | The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation. |

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, the Trust agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 22 November to 26 November. The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

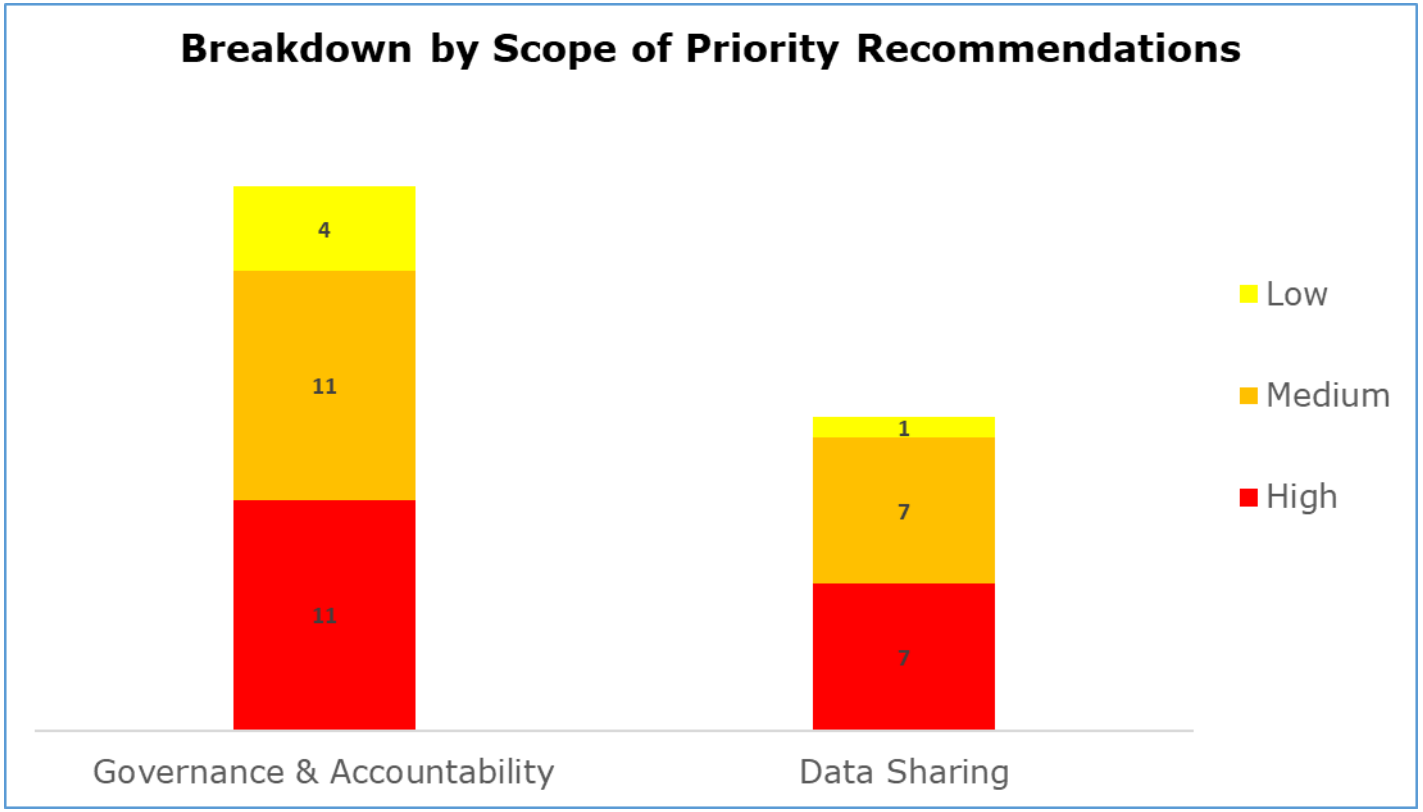
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The Trust 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. |
| **Data Sharing** | 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 at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

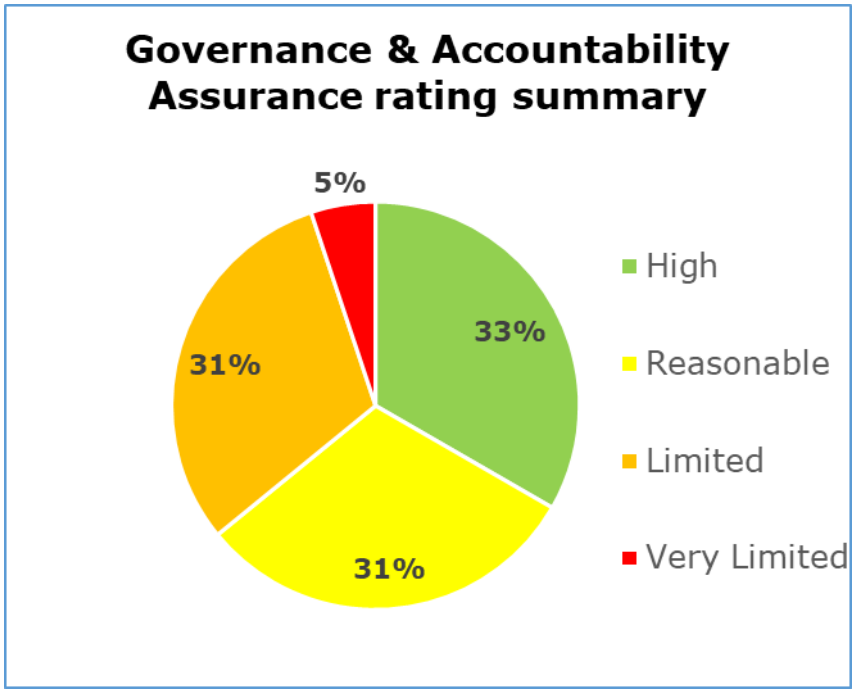
## Priority Recommendations



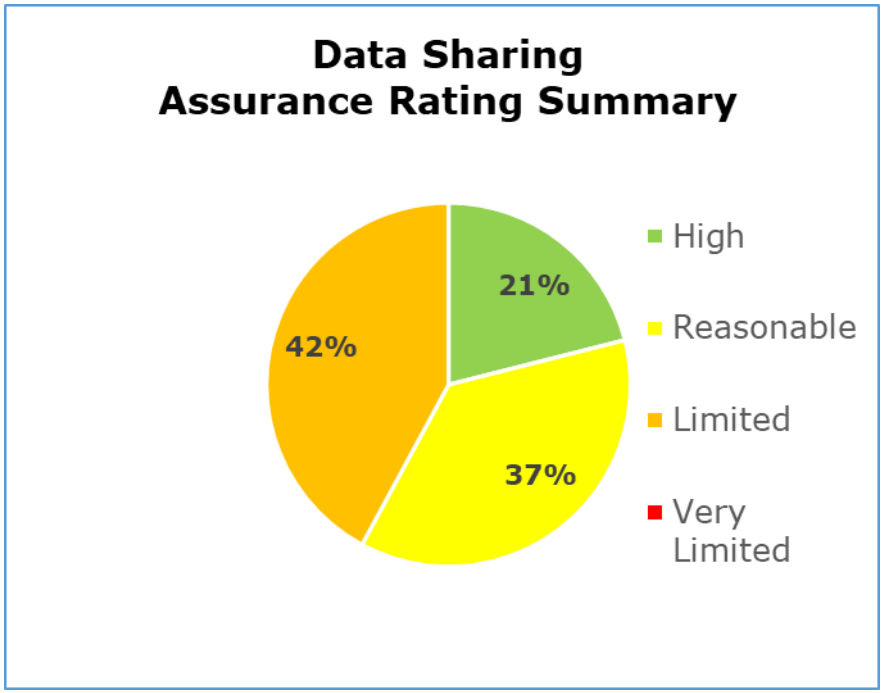

The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has 11 high, 11 medium and 4 low priority recommendations
- Data Sharing has 7 high, 7 medium and 1 low priority recommendations

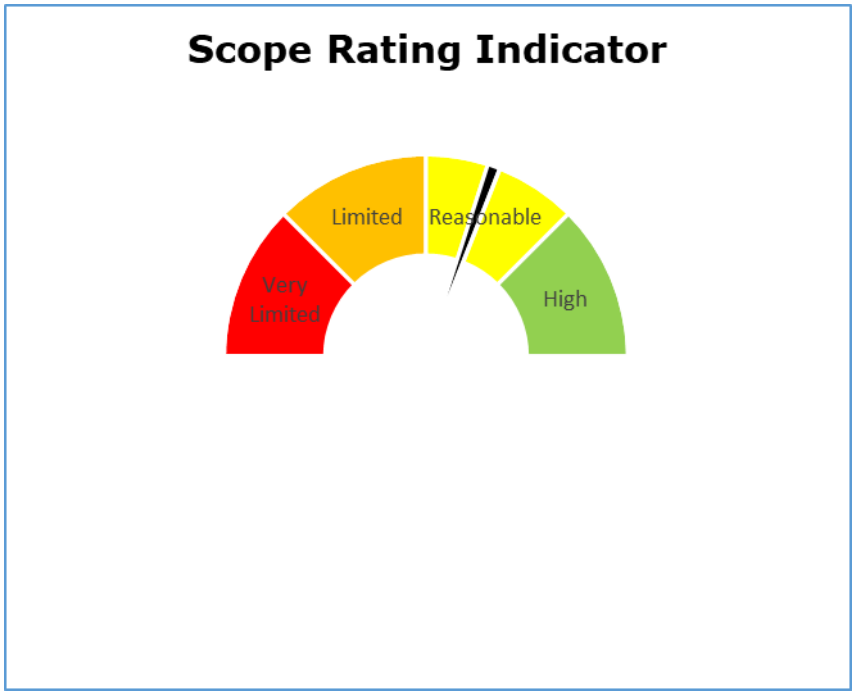
## Graphs and Charts




The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 33% high assurance, 31% reasonable assurance, 31% limited assurance, 5% very limited assurance.




The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 21% high assurance, 37% reasonable assurance, 42% limited assurance, 0% very limited assurance.




The speedometer chart above gives a gauge of where the organisation sits on our assurance rating scale from high assurance to very limited assurance.

## Areas for Improvement

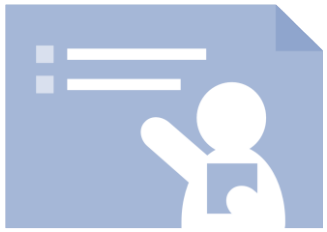
Governance & Accountability:

- The Trust's Records of Processing Activity (ROPA) needs work. What the Trust has in place is more of a data flow map and, whilst this is comprehensive, it does not include all of the requirements of Article 30 of UK GDPR.
- The Trust's DPIA screening questions and template is hard to follow and difficult to complete, this increases the risk of the template being inaccurately completed or not used at all. In addition, the DPIA screening questions do not contain all of the relevant considerations expected, such as the scope, purpose, type, and manner of proposed processing. This makes it difficult to establish the context of the new processing and for the designated reviewer to accurately review it.

Data Sharing:

- Not all staff likely to make decisions about data sharing have been identified and made aware of their responsibilities, and there is a lack of specialised training provided to staff with data sharing responsibilities both at induction as well as through periodic refresher training.
- The Trust's Information Sharing Agreement (ISA) library is not up to date and not all routine data sharing activities are covered by a sufficiently detailed ISA signed by the senior management of all sharing partners.
- Existing ISAs are not reviewed periodically, in all cases, to provide assurance that each agreement continues to operate as intended and in line with legislative requirements. The Data Performance and Assurance Group (DPAG) does not have sufficient oversight of ISA reviews as they do not feature as a standing agenda item at the DPAG's meetings.
- Sufficiently detailed policies, procedures and guidance are not in place to ensure that all staff that handle ad hoc third party disclosure requests can do so in a lawful, effective, and consistent manner.

# Credits



## ICO Audit Team

ICO Team Manager – Julie Wood
ICO Engagement Lead Auditor – Harry Evans
ICO Lead Auditor – Ben Gnatiuk

## Thanks

The ICO would like to thank Louise Eastham, Head of IG and DPO for their help in the audit engagement.

## Distribution List

This report is for the attention of Louise Eastham, Head of IG and DPO and Liz Romaniak Director of Finance and SIRO.

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