NHS Scotland Health Boards

Audit Outcomes Report

August 2023

Information Commissioner's Office

Contents

Introduction ---- 3
Scope ---- 3
Approach ---- **Error! Bookmark not defined.**
Methodology ---- 3
Overview ---- 4
Summary of Findings ---- 4
Key Findings ---- 4
Good Practice ---- 10
Conclusion ---- 12
Next Steps ---- 14
Thanks ---- 14
Appendices ---- 15
Appendix 1: NHS Scotland Health Boards audited: ---- 15
Appendix 2: Priority Ratings ---- 15
Appendix 3: Assurance Ratings ---- 16

Introduction

The Information Commissioner's Office (ICO) is responsible for enforcing and promoting compliance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations 2018 (UK GDPR). The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers. 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.

This programme was intended to assess the data protection compliance of the Scottish health boards, by conducting an audit of each board individually. The areas audited were the same for each board, so that themes could be identified. The audits took place between September 2022 and May 2023.

This report is based on our findings from our audits, focussing on the key themes identified, the recommendations we've made and the good practice we've seen.

Scope

The scope looked at a number of areas of information governance, including specialised training and data sharing, at each health board. The scope was designed to consider the extent to which information governance accountability, policies and procedures, and information sharing agreements and logs complied with the principles of data protection law.

The agreed scope of the audits was determined using existing intelligence of the data processing activities of the health boards, input from the ICO Scotland regional office, discussions with the then chair of the Health Boards' IG Forum, and attendees at the Forum itself.

Methodology

The audits were conducted following the Information Commissioner's data protection audit methodology. The key elements of this were desk-based

reviews of selected policies and procedures, interviews with selected staff, and virtual reviews of evidential documentation. A day's site visit took place for one of the audit engagements.

Each health board received an individual audit report and action plan. Where weaknesses were identified recommendations were made, in many cases to enhance existing processes to facilitate compliance with data protection law. In order to assist the boards in implementing the recommendations each was assigned a priority rating[1] based upon the risks that they were intended to address.

Overview

Healthcare in Scotland is a devolved issue, and comes under the Health and Social Care Directorates. NHS Scotland operates fourteen territorial boards across Scotland as well as seven special non-geographic boards and one public health body, employing approximately 160,000 staff. They cover all areas of public health care, including acute hospital services, mental health services, primary care, and ambulance services[2].

The territorial boards vary greatly in size and situation, from relatively small island-based boards to larger urban settings, and have their own individual considerations and challenges.

There is close collaboration between the health boards on a national and regional level, with national documents such as privacy information notices and privacy policies being adapted for local use.

Summary of Findings

The findings below summarise the key observations, opportunities for improvement and good practice seen during the programme of audits.

Key Findings

Management Structures
Effective information governance requires having clearly defined oversight and management of information.

[1] See Appendix Two for priority ratings
[2] See Appendix One for list of Health Boards audited

Evidence showed that all the health boards had a good or reasonable management framework to support their information governance function, which included having a delegated process of accountability from the Executive Board down with a Senior Information Risk Officer (SIRO) and Caldicott Guardian.

All boards had appointed a Data Protection Officer (DPO) and 88% of DPO's had appropriate responsibilities assigned, clear reporting mechanisms to senior management and operational independence. Most boards also had a framework of operational roles and responsibilities in place to support the day-to-day information governance work, and an information management steering group or equivalent to provide structure and oversight of data protection compliance at an operational level.

The audits did show however that there were some common areas where improvements could be made.

- A small number of health boards had a potential lack of resilience in the information governance function with a relatively small information governance team in place. There was a risk that not all the statutory compliance activities could be completed, such as subject access requests being responded to within the statutory period.

- In some cases, the information governance management documentation did not reflect the roles that were in place. For instance, the requirements of the role of the DPO were not described within the Data Protection Policy or the job description of the individual in that role.

- A framework of Information Asset Owners (IAOs) was not fully in place in all boards. In some cases, the IAOs were not adequately engaged in their roles in a way which enabled them to fulfil their responsibilities.

- A small number of boards did not have formal deputies in place for the Caldicott Guardian function to ensure that the tasks of this role would be carried out during absence periods.

Policies and Procedures

A framework of policies and procedures is required to support and give direction for data protection compliance.

80% of health boards had a good or reasonable policy framework in place. This comprised of a range of policies including a data protection policy, records management policy and a data sharing policy. There was an approval process in place to ensure policies and associated procedures were approved by senior management and reviewed regularly. All the boards made their policies and procedures readily available to staff, clearly signposting to them on the staff intranet pages.

The health boards may find it helpful to look at ways in which further assurance can be gained of staff having read new or revised policies, such as policy management software.

There were recommendations made in the following areas:

- Several health boards did not have approved data sharing policies in place to ensure data was shared appropriately and securely. A comprehensive data sharing policy would mitigate against the risk of unlawful sharing, personal data breaches and non-compliance with the Data Sharing Code of Practice.

- Some health boards had policies in place which had not been reviewed in line with their review dates, and therefore there was a potential risk of staff working with outdated processes. A review and approval process would provide assurance of the effectiveness of the policies and procedures.

Specialised Training

Specialised data protection training for specialised roles or particular functions should be in place to enable staff to understand and fulfil their data protection responsibilities. This is training in addition to the statutory data protection training which all staff complete.

The audits found that some health boards had limited provision for training for specialised roles such as the DPO, SIRO, IAOs and Information Asset Administrators (IAAs), as well as those involved in functions such as information security, records management and individual rights requests.

Many boards were providing specialised training on request. A number of recommendations were made identifying the need for a full Training

Needs Analysis to be carried out, in order to identify all the required data protection training throughout the organisation. Regular refresher training on a regular basis should also be built into this process.

Processor Contracts

There should be an effective framework for the processing of an organisation's personal data by a third party and this working relationship must be formalised in a written contract.

The audits showed that most of the health boards had good or reasonable procedures in place to ensure this was in place.

In most cases there were contracts in place with parties who were processing personal data on behalf of a health board and the majority of these contracts contained terms or clauses required by the UK GDPR. It is worth noting however that many contracts were nationally obtained and controlled, so the amount of contracts held by individual boards would vary greatly.

However, there were some areas of concern in a number of boards, namely:

- Around half of the boards did not have sufficient measures in place to ensure that all processors were complying with the terms of the written contract. There should be clauses included within contracts covering the right to audit to ensure processors are complying with all terms and conditions. These checks should be carried out on a regular basis.
- In around a third of the boards, the contracts were not sufficiently detailed to provide assurance that the processing required of a data processor will meet all the requirements of the law. Without this, there is a risk that the data controller will not have adequate control over the personal data processed on their behalf.
- Not all boards could offer assurance that contracts were in place with all processors handling personal data on their behalf. There must be written contracts in place to govern the work that processors are doing on behalf of the organisation, to ensure that these controls are formalised, agreed and recorded.

Transparency/Privacy Information

Organisations must be transparent about how people's personal data is processed.

We found that the majority of the health boards provided effective privacy information that was available to the public through websites, posters, leaflets or displays, and informed them how their personal data was being processed and shared.

Some improvements were recommended in certain areas, namely:

- A number of boards did not provide privacy information in a format which was aimed at children and vulnerable people, and so there was a risk that a section of their service users were unaware of how their information was processed. Some boards did have specific privacy information which had been developed for children to understand and this may be something that can be shared with others.

- In some cases boards did not provide privacy information proactively to people but relied on them accessing the website's privacy notice.

Data Protection Impact Assessments (DPIA)

Organisations must be able to identify when there is a requirement to carry out a DPIA and be able to undertake them in an effective and appropriate manner.

The audits showed that all the health boards had a good or reasonable understanding of the type of processing which required a DPIA, and all bar one had a DPIA process in place. Most boards also had an effective risk management procedure to mitigate risks identified as a result of the DPIA.

As good practice, the health boards should consider publishing their DPIAs to aid their obligations around transparency and accountability. However this needs to be balanced against risks around revealing commercially sensitive information, undermining security or other issues. It may be possible to mitigate against this by redacting sensitive details, or publishing a summary.

Areas where recommendations were made include:

- In about a third of the boards it was noted that not all relevant policies and procedures, such as the main project and change management policies and procedures, included reference to the requirement for a DPIA. This meant that recognising the need for a

DPIA was not built into the basic governance function, risking DPIAs not being undertaken when required.

- Several health boards had DPIAs that were overdue for review, or did not have a robust process for reviewing them. It is essential for DPIAs to be regularly reviewed in case of substantial change to the nature, scope, context or purposes of the processing.

Personal Data Breaches

Any breaches of personal data which occur should be handled correctly by an organisation, in order to protect peoples' rights and to meet the organisation's responsibilities under the law.

We found that 90% of boards had put in place good or reasonable means to ensure that data breaches were detected, reported and investigated effectively.

Issues that required recommendations included the following:

- Not all boards had a written process in place to determine when an individual should be notified about a data breach which was likely to result in a high risk to their rights and freedoms. We recommended that the process should include the need to document how and why the decision was made, and contain guidance and templates to ensure that the information provided to people contained all that was required to avoid a breach of the UK GDPR.

- Analysis from the ICO's Personal Data Breach team showed that a number of boards missed the target of reporting qualifying breaches to the ICO within the 72 hours required by the law. Boards must establish a process to prioritise the investigation, give it adequate resources, and expedite it urgently.

Data Sharing Agreements

Sharing personal data, often of a very sensitive nature, is a crucial part of an effective healthcare provision. But in order for it be balanced with the obligation to protect the rights of individuals there must be effective controls in place to ensure that any sharing complies with the principles of data protection law. Key to this is having appropriate and detailed data sharing agreements that are regularly reviewed.

It should be noted that the number of agreements in place at various boards differed. There is also an Intra NHS Information Sharing Agreement, a revised version of which has come into effect from July 2023. This Accord has been established to enable the sharing of personal data between NHS Scotland organisations so that they can carry out their roles in relation to providing safe patient care.

80% of the boards had data sharing agreements with all parties with whom data was routinely shared, and 95% of these agreements had an appropriate level of detail to provide effective direction to both parties and ensure that the requirements of data protection law were met.

Recommendations were made in the following areas:

- In some boards there was no log or register of data sharing agreements and in others, where one did exist, it did not contain enough details for there to be sufficient oversight of the sharing that took place.

- Data sharing practices were not always included on the organisations' data mapping and subsequent Record of Processing Activities (ROPAs), nor were categories of recipients to whom personal data was disclosed. Discussions around this area also identified that a number of boards did not have an adequate ROPA in place.

- In some cases, policy or procedural documents did not contain sufficient detail as to how agreements should be reviewed, and in others it was found that data sharing agreements did not contain review dates.

Good Practice

We were encouraged to see areas of good practice during the course of our audits. Examples of this good practice included:

Collaboration

One of the most positive elements noted in the course of the audits was that the information governance leads from the health boards had their own forum, NHS Scotland IG Leads Forum, which meets regularly for discussion, exchange of ideas and collaborative working. The boards also worked collaboratively on various projects.

This was a useful resource for the boards and offered a supportive framework through which the boards could continue to improve their compliance with data protection law. This was particularly helpful given the relative sizes of the boards and the variation in resource and experience. It also proved helpful in the development of the audit programme, as we were able to discuss the proposed audits at the forum and gained useful feedback.

Awareness & Guidance

It was notable that staff interviewed at the health boards spoke highly of their information governance departments, describing them as helpful, knowledgeable and accessible. Having effective and embedded information governance departments helped to ensure that the principles of data protection were visible and supported throughout the organisation, and provided an effective source of guidance and advice.

Data protection roles

Senior officers interviewed, such as Senior Information Risk Owners and Caldicott Guardians, showed a strong understanding of their roles in relation to information governance, which helped promote a privacy preserving culture from the top level down.

Best practice

Best practice was observed in individual boards which included:

- A wide range of supplementary privacy information tailored to the requirements of various sections of people.

- A process to ask additional questions around the conditions of processing for those situations when a DPIA was not required to ensure all processing requirements were identified.

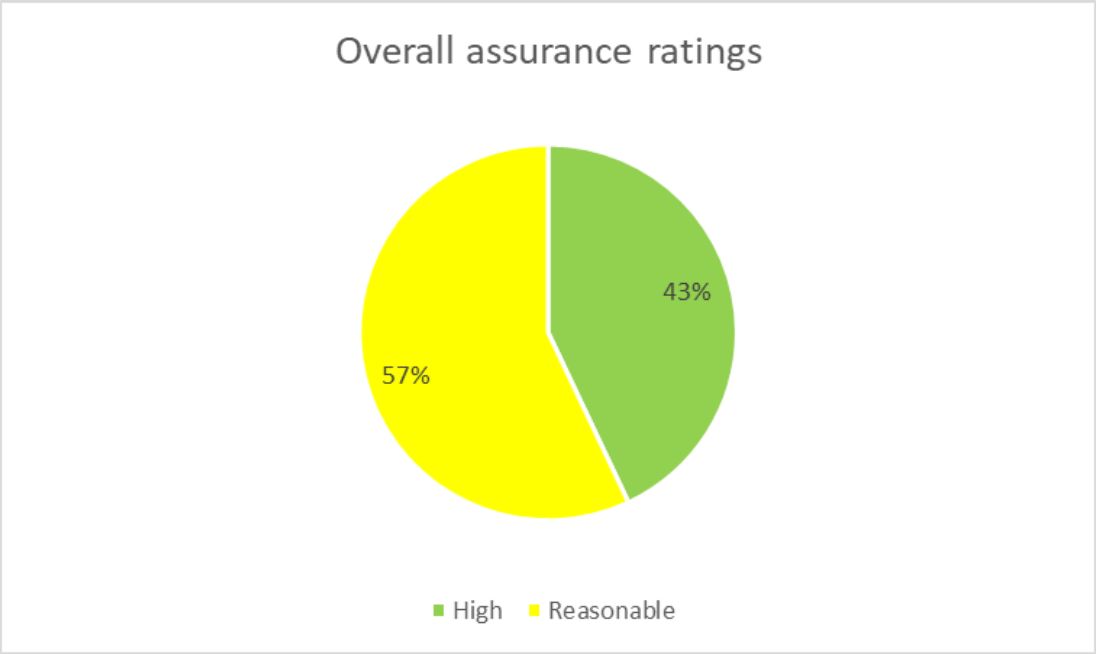
- The use of applications to construct a comprehensive Information Asset Register.

- Privacy information available where the use of printed material was not encouraged post-pandemic, such as screens displaying information in public areas.

Conclusion

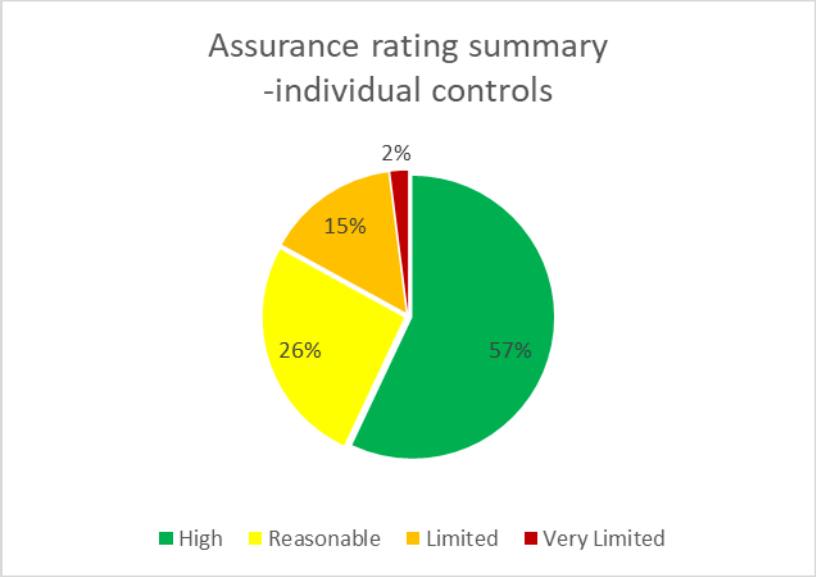
Assurance ratings

Each individual health board was given an overall assurance rating[3] at the end of their audit. **It is encouraging to note that all the boards achieved either High or Reasonable assurance** (43% and 57% respectively), as illustrated in the chart below.



In individual control areas, 57% were rated as having high assurance, demonstrating that appropriate measures were in place and effective to control the relevant risks, with no additional advice or recommendations required. The chart below illustrates all the ratings given.

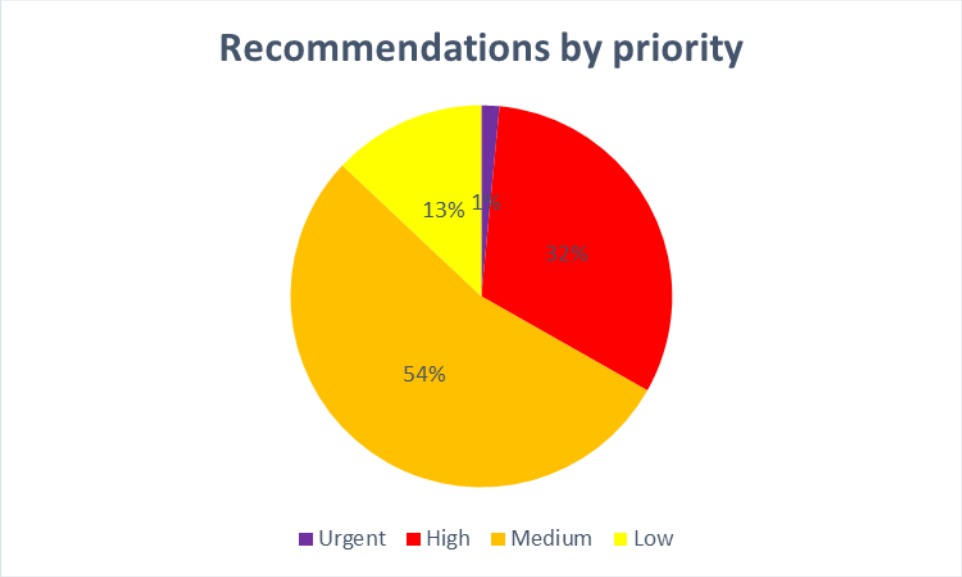
[3] See Appendix Three for assurance rating descriptions



The areas with the highest level of compliance were around transparency, management structures and policies and procedures.

Recommendations

Boards were given recommendations where weaknesses were identified. Each recommendation was given a priority rating of urgent, high, medium or low, to prioritise the areas of most risk. The chart below shows the number of recommendations made by priority.



The highest number of recommendations were medium priority (54%), followed by high priority (32%). Only one percent of the recommendations were deemed to be urgent priority, where a clear breach of data protection legislation or an imminent risk of a personal data breach were identified.

Next Steps

Following the audits all the boards agreed an action plan based on the recommendations made. They all responded positively, proposing appropriate actions to address the recommendations with suitable timelines and responsible officers identified. It was encouraging to see that many of the Boards took action swiftly to address recommendations, with some being completed shortly after the audit.

None of the audits require individual follow up, but NHS Scotland will continue to be monitored by the ICO as part of our business as usual processes.

Thanks

The Assurance team would like to thank the DPOs, Senior Information Risk Owners and other staff from the boards who facilitated the audits. The boards all demonstrated positive engagement with the audit process which is much appreciated.

Particular thanks go to Alan Bell, Head of Information Governance and DPO at NHS Grampian and chair of the NHS Scotland IG Leads Forum for facilitating discussion at the forum, and his predecessor in the role of chair, Eilidh McLaughlin, now Head of Digital Citizen Unit, Scottish Government.

Appendices

Appendix 1: NHS Scotland Health Boards audited

Healthcare Improvement Scotland
NHS 24
NHS Ayrshire and Arran
NHS Borders
NHS Dumfries and Galloway
NHS Education for Scotland
NHS Fife
NHS Forth Valley
NHS Golden Jubilee
NHS Grampian
NHS Greater Glasgow and Clyde
NHS Highland
NHS Lanarkshire
NHS Lothian
NHS Orkney
NHS Shetland
NHS Tayside
Public Health Scotland
Scottish Ambulance Service
The State Hospital

Appendix 2: Priority Ratings

Priorities are assigned as Urgent, High, Medium, or Low, on the basis of the following definitions:

Urgent – An urgent recommendation relates either to a clear breach of data protection legislation, or to an imminent risk of a personal data breach occurring if the issue is not resolved.

High – A high recommendation relates to the serious likelihood of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

Medium – A medium recommendation relates to the realistic possibility of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

Low – A low recommendation relates to the potential for a breach of the legislation or a personal data breach to occur if the issue is not resolved.

The severity of any potential consequent personal data breach is also factored into consideration when assigning a priority rating, including both the sort of data that may be part of the breach and the number of data subjects who could be affected.

Appendix 3: Assurance Ratings

Each Health Board was given an overall assurance rating, based on the following definitions:

High – There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

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.

Limited – There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Very Limited - 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.