THE STATE HOSPITALS BOARD FOR SCOTLAND

INFORMATION GOVERNANCE ANNUAL REPORT
APRIL 2024 – MARCH 2025

(Including Health Records)

Lead Author	Director of Finance and eHealth / Senior Information Risk Owner
Contributing Authors	Records Services Manager Information Governance and Data Security Officer
Approval Group	The State Hospitals Board for Scotland
Effective Date	April 2025
Review Date	April 2026
Responsible Officer	Director of Finance and eHealth / Senior Information Risk Owner

Contents

1 INTRODUCTION AND HIGHLIGHTS OF THE YEAR

The Information Governance Group is responsible for progression of attainment levels in relation to Information Governance Standards. The 2024/25 reporting year has seen continued progress in strengthening Information Governance across The State Hospital. The Group has maintained its commitment to ensuring compliance with data protection legislation, improving records management, and promoting a culture of accountability and transparency.

The Group through its regular meetings has received and scrutinised regular reports all areas of governance, including the following – RiO audits, records management, risk assessments, training, Freedom of Information (FOI), data protection and Information Governance incidents and outcomes – as well as reviewing those items on the Corporate Risk Register relevant to the Group's remit.

Key highlights from the year include:

- 100% compliance with statutory timescales for Freedom of Information (FOI) requests, alongside a 28% increase in request volume.
- Completion of 91% of the ICO audit action plan.
- Continued development of the Electronic Patient Record (EPR) system, including integration with prescribing and access approval processes.
- Introduction of a new category for Subject Access Requests to better track requests from discharged patients.
- A revised approach to policy awareness, with plans to reinstate the PC lock mechanism following a drop in engagement with the self-service portal.

Despite some challenges, including reduced meeting frequency due to workload pressures, the IGG has remained focused on delivering its objectives and adapting to evolving requirements.

This report is submitted on an annual basis to the Board, through the State Hospital's internal governance and approval structure.

The Committee has, over the course of the year continued to work to improve Information Governance standards and practices across the Hospital. We encourage staff to adopt good Information Governance standards through a number of measures undertaken by the group, and to complete mandatory online Information Governance learning modules.

2 INFORMATION GOVERNANCE GROUP

2.1 Information Governance Group membership

Director of Finance and eHealth (Chair)
Associate Medical Director/Caldicott Guardian
Head of e-Health
Head of Procurement
Clinical Admin Representative
Information Governance and Data Security Officer
Senior Information Analyst & Information Technology Security Officer
Lead Nurse
Health Records Manager
Psychology Representative
Security Information Analyst
Finance Representative
Social Work Representative
Human Resources Representative
Health Centre Representative
Pharmacist Representative
AHP Representative
Risk Management Representative
Business Manager Corporate Services
Forensic Network Representative
Information Asset Owners

2.2 Role of the group

The group has a wide-reaching remit, being responsible for all matters in respect of Information Governance within the Hospital as the title suggests. The membership of the group is purposely broad. This allows the group to be representative of staff groups and departments from across the hospital.

2.3 Aims and objectives

- Ensure compliance and development of Information Governance overall as monitored by the Data Protection Compliance Toolkit (DPCT).
- Address issues arising in the hospital in relation to Data Protection.
- Address issues arising in the hospital in relation to Records Management including structure, filing, storage, and archiving.
- Address Caldicott issues including monitoring DATIX reports and ensuring relevant training for staff.
- Provide a forum for the various staff groups within the hospital to raise any Information Governance issues and to receive feedback from Information Governance on such matters.
- To monitor requests made in relation to Freedom of Information and Data Subject Rights Requests.

2.4 Meeting frequency

The group meets on a quarterly basis to discuss any issues as outlined above, however the terms of reference include the option to hold ad-hoc meetings should the group require to meet outwith the quarterly cycle. Following agreement from the wider group, a small subgroup – the Information Governance DPCT Group – meets 6 monthly in order to concentrate on the assessment of the current attainment levels and supporting evidence required for the DPCT. In addition, another small subgroup also meets 6 monthly to review the Information Governance risk register (see para. 3.2).

2.5 Strategy and work plan

As noted in previous reports, the Caldicott principles have now been integrated within the initiatives and standards developed by NHS QIS for Information Governance. The Information Governance Toolkit and Data Protection Compliance Toolkit (DPCT) are completed twice yearly in order to monitor the performance of the hospital in relation to Information Governance.

The schedule of work for the subgroup is compiled in such a way as to allow the group to review progress with DPCT. This monitoring allows the group to develop an action plan of work to be undertaken by the group members. In addition, meetings are used to address the issues that may arise such as filing, relevant training, confidentiality issues etc..

2.6 Management arrangements

The Information Governance Group reports annually to the State Hospitals Board for Scotland through the Information Governance Group Report. The Information Governance Group also reports to the Corporate Management Team as relevant.

3 KEY PIECES OF WORK UNDERTAKEN BY THE GROUP DURING THE YEAR

3.1 Information Governance Standards

The Information Governance standards was retired at the end of 2021 and was replaced with the Data Protection Compliance Toolkit (DPCT). It has been developed from ICO's accountability framework, which supports the foundations of an effective privacy management programme. The toolkit is divided into 10 categories, within each category there are a set of statement and questions that are rated on a 1 – 4 scale

Level	DPCT Status
1	Expectations not met
2	Expectations partially met
3	Expectations met without review cycle
4	Expectations fully with review cycle

Category	Level 1	Level 2	Level 3	Level 4	Status
1. Leadership and Oversight	0%	10%	42%	48%	**Level 3**
2. Policies and Procedures	6%	35%	24%	35%	**Level 3**
3. Training and Awareness	0%	14%	24%	62%	**Level 4**
4. Individuals' Rights	17%	34%	9%	40%	**Level 2**
5. Transparency	31%	35%	19%	15%	**Level 2**
6. Records of Processing and Lawful Basis	25%	50%	25%	0%	**Level 2**
7. Contracts and Data Sharing	7%	39%	50%	4%	**Level 3**
8. Risks and DPIAs	3%	31%	28%	38%	**Level 3**
9. Records Management and Security	10%	44%	40%	6%	**Level 2**
10. Breach Response and Reporting	16%	76%	3%	5%	**Level 2**
Overall Rating (2025)	12%	39%	27%	22%	**Level 2**
Previous Rating (2024)	13%	45%	41%	1%	Level 2
Change	**-1%**	**-6%**	**+15%**	**+21%**	**=**

The DPCT shows a range of attainment with some categories showing improvement on previous levels.

Work continues in conjunction with the recommendations from ICO's audit to improve the organisations compliance status. It is also recognised that there has been improvement in some categories due to completing a review cycle as processes and polices are becoming embedded.

Changes have been made to the structure of Group meetings – rather than having full membership expected to attend all meetings, two meetings are arranged annually to have a full oversight review of the DPCT, with meetings in between with targeted attendance to focus on specific areas. In 2024-2025 the Group met in November – unfortunately due to leave and pressures of workload this was the only full meeting. However, discussions were held with relevant staff to focus on specific areas of the Toolkit, ensuring that some monitoring was carried out. Full Group meetings are scheduled to take place on 10 September 2025 and 11 March 2026.

3.2 Information Governance Risk Assessments

Information Governance risks assessments are undertaken by a subgroup of the IGG – the IG Risk Assessment Group – comprising of staff from IG, IT Security, Risk Management and eHealth as well as the Caldicott Guardian. Unfortunately there has been fewer meetings than had been planned due to other workload and absences impacting on time and resources – meetings in September and February having to be cancelled. The Group last met in December 2024 and further meetings are scheduled for 10 June 2025, 9 September 2025, 9 December 2025 and 10 March 2026.

At the meeting in December 2024 a total of twelve Information Governance risk assessments on the risk register were discussed. These covered a variety of risks (e.g. failure to communicate a change in access requests to eHealth in a timely manner and inappropriate viewing/deletion/processing of information contained in shared drives). All twelve risks are currently at or below their target risk rating of medium. A review of Datix incidents from the previous 6 months flagged up that there are some issues with the internal mail service and with staff sending emails to the wrong email address. New risk assessments will be completed for these issues. A number of Datix reports were noted to be in relation to slow response to FairWarning alert emails and this has been raised through OMT.

The Risk Assessment Group continues to work through registered risks to update them to reflect new technologies and working practices such as Teams and remote working. The Group continues to work to be proactive rather than reassessing out of date risks and this is proving to be beneficial.

3.3 Information Governance Training

The majority of Information Governance training is delivered online through the LearnPro platform. All training modules are mandatory for all staff members. Completion rates are monitored by the Training & Professional Development Manager, with oversight provided by the Information Governance Group (IGG).

The table below shows completion rates for each module over the past four years:

Module	Mar 2022	Mar 2023	Mar 2024	Mar 2025
IG: Essentials (Target >80%)	76%	95%	85%	75%
IG: Series (Target >85%)	-	-	87%	93%
Confidentiality	98%	98%	-	-
Data Protection	97%	98%	-	-
Records Management	98%	98%	-	-

In 2024, the Confidentiality, Data Protection, and Records Management modules were reviewed and updated. Following this review, they were consolidated into a new combined module known as the IG: Series. This change has streamlined reporting and reflects a more integrated approach to staff training in key areas of information governance.

3.4 Category 1 & 2 Investigations

There were no Category 1 or Category 2 investigations relating to Information Governance during the year.

3.5 Personal Data Breaches

Under the UK General Data Protection Regulation (UK GDPR), organisations are required to record all personal data breaches. Where a breach poses a high risk to the rights and freedoms of individuals, it must be reported to the ICO within 72 hours of discovery.

At the State Hospital, all potential personal data breaches are recorded using the Datix incident management system. The table below summarises the number of breaches recorded and those reported to the ICO over the past four years:

	2021/22	2022/23	2023/24	2024/25
Reported Breaches	56	35	24	16
Notified to ICO	0	0	0	1

In 2024/25, 14 of the 16 recorded breaches were attributable to The State Hospital, representing a continued year-on-year reduction. Two incidents were not attributable to the organisation:

Incident 1: Involved Occupational Health files affected by a cyber incident at NHS Dumfries and Galloway. Due to the potential severity, this was reported to the ICO within the required 72-hour timeframe. The ICO confirmed that The State Hospital was not responsible for the information affected by the breach.

Incident 2: Reported by the Mental Welfare Commission (MWC), this involved the loss of CPA and SPO1 documents for a State Hospital patient by an individual carrying out work on behalf of the MWC. The MWC reported the incident to the ICO. As the breach did not originate within The State Hospital, it was logged for record-keeping purposes, and no further action was required.

Area	Percentage
Internal Email Disclosures	36%
Information Disclosed Internally (non-email)	29%
Information Disclosed Externally	21%
Others	14%

The majority of breaches involved communication channels, particularly email and physical post.

The State Hospital continues to promote high standards of Information Governance across the organisation. Staff are regularly reminded of best practices through guidance shared in the Staff Bulletin, and Information Governance Walkrounds provide opportunities for informal engagement and on-the-spot advice.

3.6 Electronic Patient Records

The Electronic Patient Record (EPR) RIO, has continued to be further developed since the major upgrade in March 2022. The project specific RIO Group continue to meet on a weekly basis to ensure developments are progressing well, and to resolve any issues that have arisen or been reported. A multidisciplinary project approval group (Rio Oversight and Development (ROAD) Group) continues to meet monthly to review ongoing requests to improve RIO as well as look at future developments. A further upgrade was successfully made to the system in October 2024.

Regular audits continue to be carried out on various areas within Rio, with documentation and guidance updated as required. Issues are discussed at the Information Governance Group, or the ROAD Group.

A robust system is in place for Requests for Change to RiO – this may involve a quick assessment and authorisation by the system owner, or a more thorough review by members of the team including IG checks and workability.

RIO is now fully integrated with the medication prescribing system (HEPMA) and processes such as for grounds access approval and now embedded in the system. A large piece of work which is still ongoing is the integration of the CPA process and documentation with Rio. This is planned for live testing in April/May

3.7 Information Governance Walkrounds

Introduced in 2015 as a recommendation from the NHS Scotland Information Assurance Strategy (CEL 26, 2011), Information Governance Walkrounds have continued to build on their success in previous years. These unannounced visits take place at random intervals throughout the year and cover all areas of the organisation where personal information is handled.

Walkrounds are assessed using a consistent grading system to ensure comparability across visits:

Grade	Description
Excellent	No issues found
Very Good	1 – 3 minor issues found
Good	4 – 8 minor issues and/or 1 significant issue found
Improvements needed	9 - 14 minor issues and/or 2 significant issues found
Action Plan required	more than 15 minor issues, more than 2 significant issues and/or 1+ suspected breaches of legislation

Staff conducting the walkrounds consistently observed high standards of Information Governance across the organisation.

During the reporting year, 11 areas were inspected. Of these, nine were graded ‘Good’ or better, with the majority achieving a ‘Very Good’ rating. Two areas were assessed as ‘Improvements Needed’, but all identified issues were promptly addressed following engagement with the relevant staff and managers.

Walkrounds complement the organisation’s Records Management Plan and broader Information Governance objectives. They also provide an informal and supportive opportunity for staff to ask questions, seek clarification, and increase their awareness of good information handling practices.

3.8 FairWarning

The Group receives exception reports detailing the volume and nature of FairWarning alerts, which monitor access to personal information. A dedicated subgroup is responsible for maintaining appropriate alert thresholds to ensure a proportionate and effective audit process.

Overall, alert levels remained consistent with previous years, taking into account fluctuations in the patient population. A continued increase in alerts related to multiple staff accessing a single patient’s record within a single day was observed. Upon review, this trend was attributed to changes in clinical practice. As a result, the trigger point for this alert was adjusted to reduce notifications generated by routine and appropriate access.

The Group remains satisfactorily assured that there are no concerns regarding inappropriate access to personal information.

3.9 Records Management

This year has again been extremely busy but positive for the Records Services Department. Staff have undertaken work in three separate areas – health records, records management and information governance – which has been challenging at times however staff have undertaken this change in workload well. However, it has been noted that as all of these areas are growing due to additional legislation and expectation on the organisation, it may be better to focus staff on specific areas of expertise and this was put in place in January 2025. The first three months of this went well, and a more permanent way of handling workload will be explored in 2025.

The State Hospitals Board for Scotland submitted its first Records Management Plan (RMP) to the Keeper of the Records in December 2016. The Plan was agreed and accepted by the Keeper with some elements graded as amber, and having work outstanding. As records management has changed and become more at the forefront in the State Hospital, a new RMP was submitted to the Keeper of the Records of Scotland in December 2024. This work was carried out with input from various disciplines throughout TSH led by the Records Services Manager, with a large volume of evidence being submitted. There is a known backlog of Plans awaiting assessment by the Keeper therefore a response is not expected before June 2025.

The Records Management Group was responsible for the oversight of the resubmission of the RMP as well as meeting to discuss other records issues. There have been no meetings since December 2024 due to staff absence, however future meetings are scheduled with one of the main tasks being to work on the introduction of the National Business Classification Schedule (BCS) to TSH. The BCS will also be a foundation of the move to using MS SharePoint therefore it is important that this structure becomes familiar to staff.

3.10 Freedom of Information

The Information Governance Group continues to receive regular updates on all Freedom of Information (FOI) requests, including performance against statutory response times. In 2024/25, the number of FOI requests increased by 28% compared to the previous year.

The majority of requests originated from the general public (37%), followed by businesses (18%) and the media (17%).

Number of Freedom of Information Requests

	2020/21	2021/22	2022/23	2023/24	2024/25
Requests made	262	172	145	242	310
Completion rate within timescales	89%	99%	91%	95%	100%

In 2024/25, 100% of FOI requests were responded to within the statutory timeframe, reflecting a strong commitment to transparency and accountability.

Where information was held, a full response was provided in 76% of cases.

Number of Freedom of Information Reviews

	2020/21	2021/22	2022/23	2023/24	2024/25
Requests for review made	3	4	2	1	1
Upheld without modification	3	4	2	1	1
Upheld with modification	0	0	0	0	0
Substituted a different decision	0	0	0	0	0
Reached a decision where no decision had been reached	0	0	0	0	0

The number of FOI reviews remained consistent with the previous year, with one review conducted in 2024/25. The review concluded that the original response issued by the State Hospital was appropriate and required no changes.

3.10.1 Freedom of Information Self-Assessment

The FOI Committee continues to lead a cycle of continuous improvement, guided by the Scottish Information Commissioner's self-assessment toolkit. This toolkit supports public authorities in evaluating their performance across six key areas of FOI compliance.

Each module is assessed using a four-point scale:

Ratings	**Meaning**
Excellent	Greatly exceeds the requirements of FOI
Good	Exceeds the requirements of FOI
Adequate	Meets the requirements of FOI
Unsatisfactory	Below the requirements of FOI

Public authorities, including The State Hospital, are expected to achieve at least an 'Adequate' rating, taking into account their specific operational context.

Standards and Criteria	**2021/22**	**2022/23**	**2023/24**	**2024/25**
1. Responding on time	Good	Good	Excellent	Excellent
2. Searching for, locating and retrieving information	Good	Good	Good	Good
3. Advice and assistance	Adequate	Good	Good	Good
4. Publishing information	Adequate	Adequate	Adequate	Adequate
5. Conduct of Reviews	Good	Good	Good	Excellent
6. Monitoring and managing FOI performance Standards and Criteria	Good	Good	Good	Good
Overall	Adequate	Adequate	Good	Good

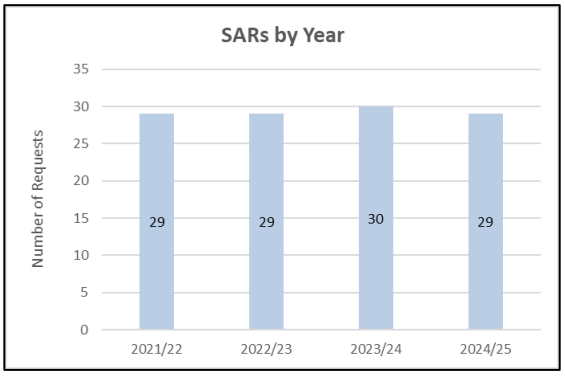
The 2024/25 assessment confirms that FOI management within the organisation now exceeds the statutory requirements of the Freedom of Information (Scotland) Act.

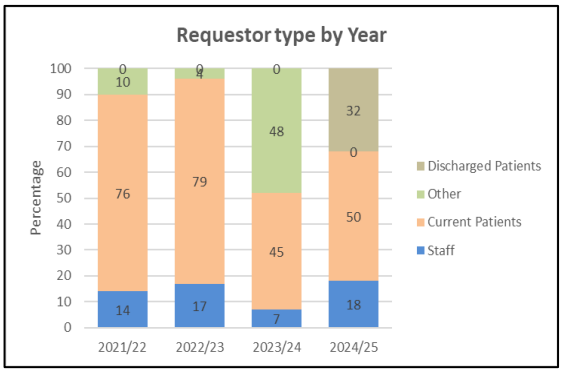
While the overall rating is typically determined by the lowest score across the six modules, the assessment framework allows for local context to be considered. In particular, the criteria for Publishing Information assumes stakeholders have ready access to information and services that are not appropriate in a high-security hospital setting. As such, provided this module is not rated 'Unsatisfactory', it is excluded from the overall rating calculation.

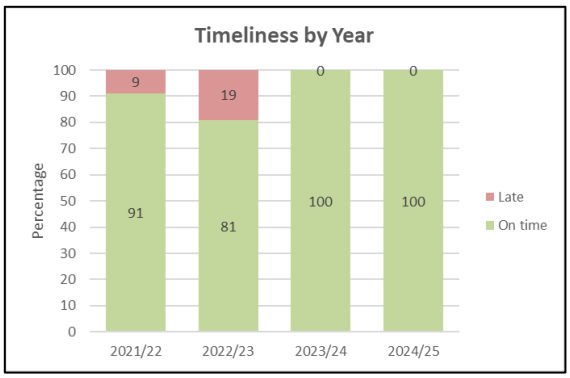
3.11 Subject Access Requests

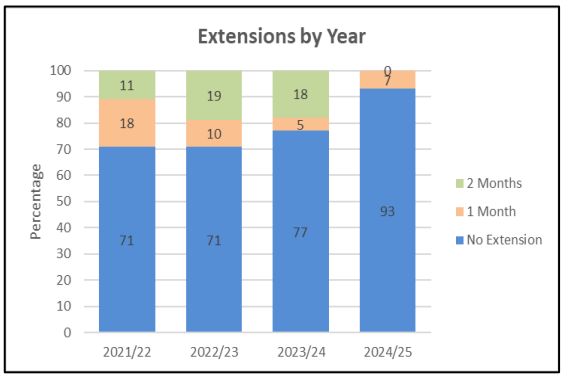
The volume of Subject Access Requests (SARs) received during 2024/25 remained consistent with previous years and within expected levels. The organisation maintained its strong performance in responding to all requests within the statutory timescales, while also achieving a reduction in the number of extensions required to complete responses. This reflects ongoing improvements in internal processes and resource management.

Following an observation in the previous reporting year that a significant proportion of SARs were being submitted by discharged patients, a new category was introduced to specifically record and monitor these requests.









3.12 MetaCompliance / MyCompliance

In 2024/25, the organisation transitioned from the legacy MetaCompliance platform to MyCompliance as its new policy awareness system. This platform was introduced to ensure that all staff are informed of key organisational policies, with the aim of supporting understanding and compliance across the workforce.

It was anticipated that the self-service portal within MyCompliance would offer a more user-friendly and less disruptive experience—allowing staff to review and acknowledge policies at their convenience, rather than through the previous method which locked users' PCs until policies were accepted.

However, uptake of the self-service approach was significantly lower than expected. As a result, staff policy awareness dropped to 39%, a sharp decline from 93% the previous year.

In response to this outcome, the Policy Approval Group decided to reinstate the PC lock mechanism in the upcoming reporting year, aiming to improve staff engagement and ensure greater compliance with policy acknowledgements.

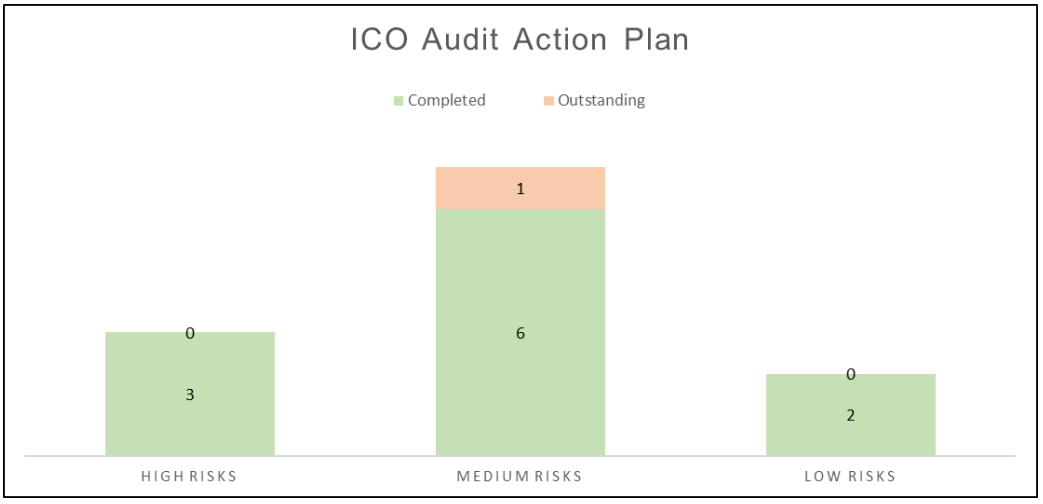
4 INFORMATION COMMISSIONER'S OFFICE AUDIT

In November 2022, The State Hospital underwent an audit by the Information Commissioner's Office (ICO). The purpose of the audit was to assess:

- The organisation's compliance with data protection legislation,
- Its use of ICO guidance and best practice resources, and
- The overall effectiveness of its data protection governance and activities.

The audit concluded with a high assurance rating, reflecting a strong level of confidence in the hospital's data protection practices.

While the findings were largely positive, the ICO identified several areas for improvement. In response, and in consultation with the ICO, the hospital developed a 12-point action plan to be implemented over a two-year period.



As of this reporting year, 91% of the action plan has been successfully completed, with only one action remaining. The outstanding item relates to the training of Information Asset Administrators, and work is currently underway to schedule these training sessions

5 IDENTIFIED ISSUES AND POTENTIAL SOLUTIONS

During the reporting year, several challenges were identified that impacted the delivery and oversight of Information Governance activities. These include:

- Reduced frequency of IG Risk Assessment Group meetings, due to staff absences and availability.
  A revised meeting schedule has been agreed for 2025/26 to ensure regular risk reviews are maintained.
- Initially low engagement with the newly-introduced MyCompliance self-service portal, resulting in a significant drop in policy awareness.
  The previous method of locking PCs will be reinstated
- Delays in progressing some elements of the ICO action plan, particularly around Information Asset Administrator training.
  Training sessions are currently being scheduled with the relevant staff to address this final outstanding action.
- Challenges in managing growing workloads across Records Services, due to increasing legislative and operational demands.
  A new staffing model was introduced in January 2025 to allow staff to focus on specific areas of expertise, with early results showing positive outcomes.
- Emerging risks related to internal communications and email errors, identified through Datix incident reviews.
- New risk assessments are being developed, and awareness-raising measures are being implemented through staff bulletins and IG Walkrounds.

The IGG remains committed to addressing these issues proactively and ensuring that robust governance arrangements are in place to support safe and effective information handling across the organisation.

6 FUTURE AREAS OF WORK AND POTENTIAL SERVICE DEVELOPMENTS

Work / Service Development	Timescale
Robust system to be in place to submit statistical returns to Public Health Scotland	July 2025
Further implementation of national Business Classification Schedule in shared drive areas	December 2025
Utilisation of software assisted redaction for subject access requests for clinical records	June 2025
Reconfiguration of MyCompliance	October 2025
Maintain 80% completion for the IG: Essentials learning module.	Ongoing
Maintain 85% completion for the IG: Series learning module.	Ongoing

7 NEXT REVIEW DATE

April 2026