THE STATE HOSPITALS BOARD FOR SCOTLAND

INFORMATION GOVERNANCE ANNUAL REPORT

APRIL 2023 – MARCH 2024

(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
	Associate Medical Director / Caldicott Guardian
Approval Group	The State Hospitals Board for Scotland
Effective Date	April 2024
Review Date	April 2025
Responsible Officer	Director of Finance and eHealth / Senior Information Risk Owner

Table of Contents

1 INTRODUCTION AND HIGHLIGHTS OF THE YEAR

The Information Governance Group, chaired by the Senior Risk Information Owner (SIRO) is responsible for progression of attainment levels in relation to Information Governance Standards.

These are recorded and monitored through the Data Protection Compliance Toolkit (DPCT). The Caldicott Guardian principles are fully integrated within the initiatives and standards required for Information Governance

The Group through its quarterly 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.

In addition, there has been a focus on monitoring the progress of the 12 follow-up actions arising from the 2022 audit by The Information Commissioner's Office (ICO) – which had received an overall rating of "High" ("a high level of assurance that processes and procedures are in place and are delivering data protection compliance"). The audit focussed on organisational structure, policies and procedures, training for specialist IG roles, transparency, contracts with contractors and data breaches – and all actions are complete or on schedule.

During 2023/24, Information Governance support and assistance was also provided to the team responsible for preparing the Hospital's submission to the Network & Information Systems (NIS) Audit – which was completed in December 2023 and resulted in a compliance rating of 76%, "showing strength across the organisation and a high level of performance".

We have also continued to adhere to recommendations included in the Scottish Government's "NHSScotland Information Assurance Strategy CEL 26 (2011)" document and the regular schedule of Information Governance walkrounds within the Hospital has continued, including non-patient areas. In addition, the group has continued to focus on other key areas of priority such as the electronic patient record (EPR) system and outcomes of the FairWarning system – together with any ad hoc issues such as record retention and email scams.

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 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%	42%	58%	0%	**Level 3**
2. Policies and Procedures	6%	47%	47%	0%	**Level 2**
3. Training and Awareness	5%	14%	81%	0%	**Level 3**
4. Individuals' Rights	20%	34%	46%	0%	**Level 2**
5. Transparency	31%	50%	19%	0%	**Level 2**
6. Records of Processing and Lawful Basis	25%	50%	25%	0%	**Level 2**
7. Contracts and Data Sharing	7%	39%	54%	0%	**Level 3**
8. Risks and DPIAs	3%	45%	52%	0%	**Level 3**
9. Records Management and Security	13%	44%	41%	2%	**Level 2**
10. Breach Response and Reporting	16%	76%	8%	0%	**Level 2**
Overall Rating (2024)	**13%**	**45%**	**41%**	**1%**	**Level 2**
Previous Rating (2023)	15%	49%	36%	0%	Level 2
Change	**-2%**	**-4%**	**+5%**	**+1%**	**=**

Whilst the DPCT shows a range of attainment, this year's position was due to the implementation of a new method of monitoring compliance.

Work continues in conjunction with the recommendations from ICO's audit to improve the organisations compliance status.

There has been a slight improvement noted in the scoring of the DPCT monitoring areas. Some of this is in part to a change that has been made to the way the meetings of the Group are held – 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.

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 impacting on time and resources. The Group last met in February 2024 and further meeting is planned for August 2024.

At this time there were four open Information Governance risk assessments on the risk register covering a variety of risks (e.g. failure to communicate a change in access requests to eHealth in a timely manner). All four risks are currently at or below their target risk rating of medium. A review of Datix incidents from the previous 6 months flagged up the requirement for reminders to be sent to staff re the importance of checking email addresses prior to sending. No new risk assessments were felt to be required at that time.

On each occasion that the Information Governance risk assessments have been updated steps have been taken to minimise the risks highlighted (e.g. procedures to ensure identifiable information is sent recorded delivery; procedures re mobile devices; risks associated with staff leaving the organisation).

The Risk Assessment Group is currently working through registered risks to update them to reflect new technologies and working practices such as Teams and remote working. Reports are now provided to the group on all relevant incidents recorded through Datix and the DPO register of personal data breaches. The Group has changed its working methodology 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 for staff is delivered online via LearnPro. All modules remain mandatory for all staff. Monitoring of completion rates by staff is undertaken by the Training & Professional Development Manager, with oversight by the IGG.

The completion of the modules can be seen in the table below.

Module	Mar 2021	Mar 2022	Mar 2023	Mar 2024
IG: Essentials (Target >85%)	78%	76%	95%	85%
IG: Series (Target >80%)	-	-	-	87%
Confidentiality	98%	98%	98%	-
Data Protection	98%	97%	98%	-
Records Management	98%	98%	98%	-

The changes have been made to the reporting of the Confidentiality, Data Protection and Records Management modules following their review and update last year. These modules are known collectively known as the IG: Series.

3.4 Category 1 & 2 Investigations

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

There was one Category 2 investigation which related to an external email address being included in an internal email distribution group that lead to confidential patient information being inadvertently disclosed to a third party.

The investigation recommended that:

- Email Distribution groups have only one owner.
- Regular checks are made to ensure group memberships continue to be appropriate
- Raise staff awareness about checking email addresses added to distribution groups.
- Raise awareness of other secure methods of data transfer, such as secure file transfer or direct upload to digital systems like RiO.

3.5 Personal Data Breaches

Under the UK GDPR there is a requirement to record personal data breaches. In cases where there is a high risk to the individuals involved, these breaches must be reported to the Information Commissioner's Office no later than 72 hours from discovery. The State Hospital uses Datix to record potential breaches of personal data which are shown below:

	2020/21	2021/22	2022/23	2023/24
Reported Breaches	19	56	35	24
Required ICO Notification	0	0	0	0

There were 24 recorded personal data breaches in 2023/24 that were attributable to The State Hospital, which is a reduction over last year.

Area	Percentage
Internal Email Disclosures	29%
Information Disclosed Externally	25%
Others	17%
Information Disclosed Internally (non-email)	13%
Leak to the Media	8%
Incorrect Information	4%
Information Unavailable When Needed	4%

The majority of recorded breaches related to our communication platforms (email and physical post).

We continue to encourage staff as to the importance of displaying high standards in relation to Information Governance. Guidance notes are circulated through the Staff Bulletin and Information Governance Walkrounds provide an opportunity for informal contact with staff to give guidance on Information Governance matters

No breaches required notification to the Information Commissioner's Office (ICO).

3.6 Electronic Patient Records

Members of the IGG were actively involved in the ongoing development of the EPR (RiO) – and the project-specific EPR Group continues to meet regularly. RiO 22 went live on 08 March 2022 with a successful transition period. Following this we have moved quickly to introduce BAU process for ongoing development of RiO. A multidisciplinary project approval group (Rio Oversight and Development (ROAD) Group) has been established that reports to the eHealth Sub Group. Included within the approval process is appropriate information governance scrutiny.

Regular audits are 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.

Further work has been carried out to integrate links between RiO and the medication prescribing system (HEPMA) – a link for users from RiO to HEPMA is under development. A substantial piece of work for the RiO project team over the last period has been the development of Grounds Access processes embedded in RiO. These went live in June 2024. Since then the feedback in relation to this development has been extremely positive, with feedback that the new system has substantially improved the timescales from application to granting.

3.7 Information Governance Walkrounds

Having been introduced in 2015 as a recommendation following the publication of the NHS Scotland Information Assurance Strategy CEL 26 (2011) the Information Governance Walkrounds have built on the success of the previous years. The unannounced walkrounds occur a random throughout the year and encompass all areas of the organisation were personal information is used.

At the start of this year a new system of recording was introduced to promote more consistency during walkrounds.

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

The staff members involved in walkrounds noted the good standards of Information Governance that have been apparent in visited areas.

Of the eleven areas inspected during the year, nine were graded good or better, with the majority being ‘Very Good’. Two areas required improvement, however all issues were promptly resolved after communication with the relevant staff members and managers.

The walkrounds compliment the Records Management plan and general information governance goals by providing an informal opportunity for staff to raise questions or seek guidance on specific aspects of their work as well as raising general awareness of information governance considerations.

3.8 FairWarning

The group receives exception reports on the levels of FairWarning alerts raised and a subgroup is tasked with maintaining appropriate alerts and thresholds to provide a proportionate audit of access to personal information.

In the main FairWarning alerting rates remained consistent with previous years taking in to account changes in the patient population over the year. However, there has been a notable increase in the number of alerts relating to high numbers of staff accessing a single patient's record in one day. Whilst all the alerts were appropriately closed, if the trend continues the subgroup may need to review the cause of this increase in alerts.

This is the eighth consecutive year in which no incidences of inappropriate access have been alerted via FairWarning.

The group continues to be satisfactorily assured that there are no areas of concern regarding inappropriate access.

Whilst the focus of FairWarning is to detect potential inappropriate access to patient records, the sustained absence of such actions from any area of the organisation should be seen as a very positive statement about the professional conduct of staff.

3.9 Records Management

This year has again been extremely busy but positive for the Health Records Department. The addition in staffing resources has meant that day-to-day workload is mostly manageable and there has been some advances made in the wider Records Management workload.

The State Hospitals Board for Scotland submitted its 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. A Plan Update Review (PUR) was carried out and submitted to National Records of Scotland (NRS) in October 2021. A positive response to this was received in December 2021, recognising the work that has now been carried out in areas such as the creation of a Corporate Records Policy and a formal Information Asset Register. As there have been noted improvements in Records Management within the organisation, it has been agreed with the NRS team that a full resubmission of the RMP will be completed in December 2024. A project group consisting of staff from around the organisation is working on this..

The move to a separate service (Records Services Department) is well underway, with a more formal split from eHealth taking place. This is allowing the department to function more independently and become involved in projects and work around the hospital, liaising with staff from various departments to promote RM in all areas. Staff are becoming more confident in dealing with corporate records as well as maintaining day to day oversight of clinical records.

The Records Management Group has met and is responsible for oversight of the resubmission of the RMP. A sub-group of the IGG is also being formed with responsibility for the oversight of clinical records – this was set to meet for the first time in Summer 2023, however due to lack of clinical input, this was not achieved. A further attempt will be made in Autumn 2024. A Quality Improvement project to reduce data held in shared drive space, and also to being using a Business Classification Scheme had begun, although due to resource issues this is now being taken forward as part of the RMP and Information Asset Register work rather than a QI project.

The current Health Records Policy and Corporate Records Policy are going to be merged to form an overarching Records Management Policy in Summer 2024. A formal Retention and Destruction Policy was agreed in September 2023, and work is ongoing with regard to formal guidance on version control and naming conventions..

Appraisal of patient records for permanent preservation or destruction has continued, with more records having been destroyed. Referral files have also been appraised as part of this process.

Work is ongoing to gather metadata on items for permanent preservation with the National Records of Scotland.

Work is being undertaken in relation the to the Hospital's Information Asset Register. This includes staff recording data as well as assisting staff to complete the process of registering systems and data held, whilst offering advice and encouragement to incorporate records management methodology. A formal records survey has been restarted however this has been slow to move forward due to resource issues. More time will be put into this in Summer 2024 in line with the RMP resubmission.

Work relating to M365 is still ongoing with the Records Service Manager being involved in national groups to ensure good RM is included in all areas and to ensure the organisation is aware of what is taking place outwith our own organisation. There is also national work to update the Records Management Code of Practice ongoing which the Health Records/Records Services Manager has contributed to. Information and updates from this work is shared regularly with internal colleagues.

As 2023 celebrated the 75th birthday of the NHS, the department put on a display of historical artefacts and information relating to changes in how The State Hospital has developed throughout the years in the Wellbeing Centre. This was positively received, with many staff coming along to view photographs and other memorabilia. As this generated interest, it has been agreed that departmental staff will provide an introduction to TSH at staff inductions, to give new colleagues an idea of the history of the Hospital.

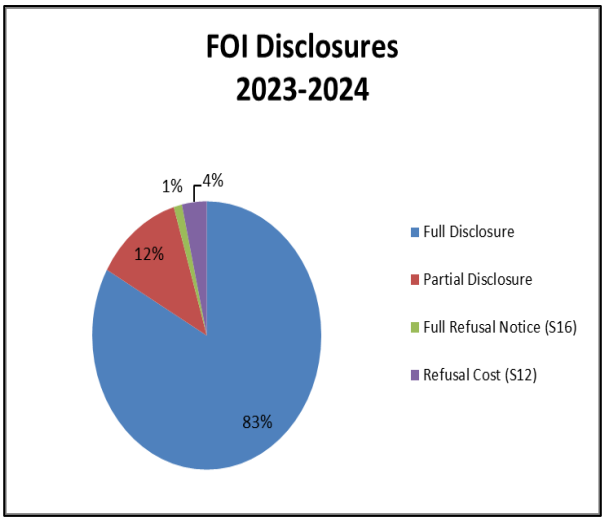
3.10 Freedom of Information

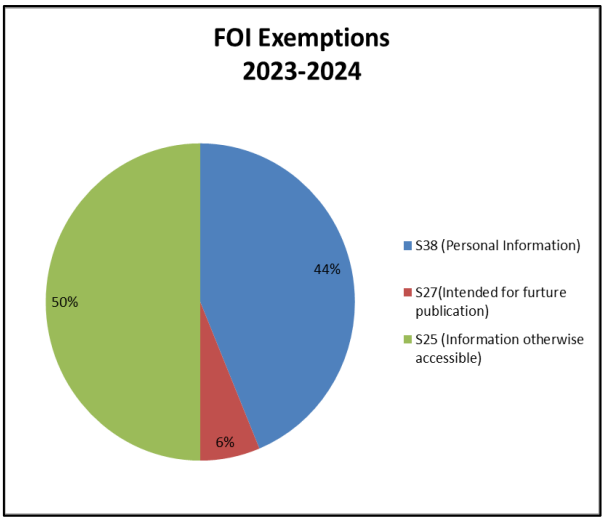
The group is kept informed of all Freedom of Information (FOI) requests and of the timescales achieved in responding to these. Requests have mainly come from the general public (64%), with the charities, lobby or campaigning groups (14%) the second largest requestors. The numbers of requests (shown below) were up 66% over last year.

	2019/20	2020/21	2021/22	2022/23	2023/24
Requests made	224	262	172	145	242
Completion rate within timescales	100%	89%	99%	91%	95%

This year has seen another drop in requests for reviews (shown below), with all the reviews finding that The State Hospital's original response was an appropriate response, which required no modification.

	2019/20	2020/21	2021/22	2022/23	2023/24
Requests for review made	0	3	4	2	1
Upheld without modification	0	3	4	2	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





Where the organisation held information, it provided a full response to applicants for the majority of requests (83%).

Three exemptions were used to withhold or decline to publish information. In most cases (50%) this was because the requests related to information that the applicant could reasonably obtained without making a FOI request.

3.10.1 Freedom of Information Self-Assessment

The FOI Committee drive a continuing improvement cycle based on the Scottish Information Commissioner's self-assessment toolkit.

The toolkit comprises of six modules each reviewing a particular area of our FOI obligations providing a four-point scale of performance (Unsatisfactory, adequate, good and excellent) that reviews the year's performance. Modules 5 & 6 were introduced by the Commissioner in 2021/22.

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, such as The State Hospital, are expected to deliver an 'adequate' service, taking in to account their local setting.

Standards and Criteria	2020/21	2021/22	2022/23	2023/24
1. Responding on time	Good	Good	Good	Excellent
2. Searching for, locating and retrieving information	Good	Good	Good	Good
3. Advice and assistance	Adequate	Adequate	Good	Good
4. Publishing information	Adequate	Adequate	Adequate	Adequate
5. Conduct of Reviews	N/A	Good	Good	Good
6. Monitoring and managing FOI performance Standards and Criteria	N/A	Good	Good	Good
Overall	Adequate	Adequate	Adequate	Good

The assessment shows that the management of FOI with the organisation now exceeds the requirements of the Freedom of Information (Scotland) Act.

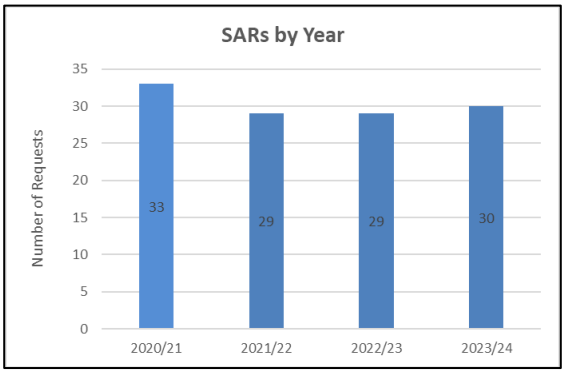
The overall rating is usually determined by the lowest score over the six sections, however the assessment allows for local circumstances to be considered when calculating the rating.

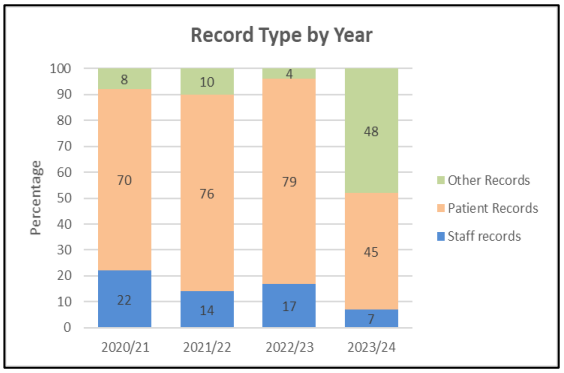
The criteria for scoring the fourth module about publishing information makes assumptions about FOI stakeholders which cannot be applied to our patients due to nature of a high security environment.

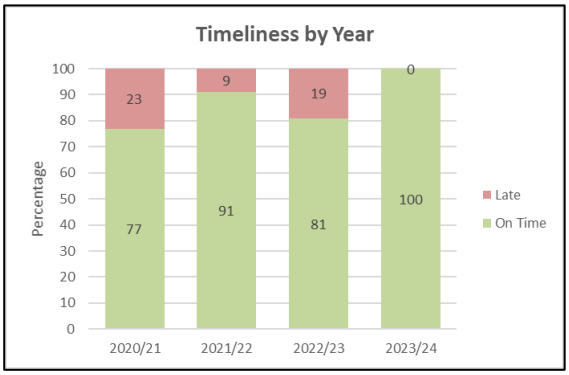
As such, provided that the rating for this section is not 'Unsatisfactory', it will be disregarded when calculating the overall ratings going forward.

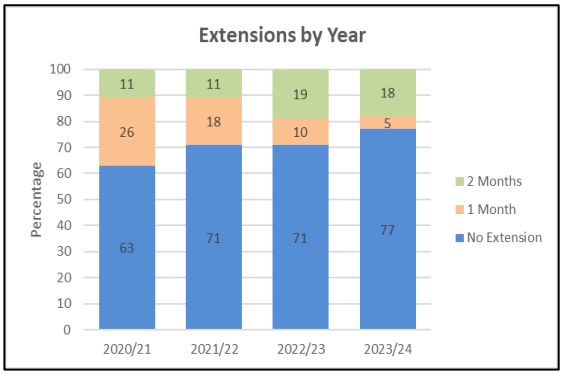
3.11 Subject Access Requests

Subject access requests continue at expected numbers, although there has been a notable change in who makes requests. Previously the majority of requests came from our current patients, however the majority of requests (48%) this year were received from discharged patients.









3.12 MetaCompliance / MyCompliance

MetaCompliance is a policy management system which is designed to ensure that key policies are communicated to all members of staff in order to ensure they obtain, read and understand their content. It also provides evidence of communication to line management and can identify individual staff members as having read and understood key policies.

MetaCompliance is supported by the complimentary system MyCompliance which provides a way to acknowledge policies prior to MetaCompliance enforcing a response.

Over the last year the number of policies delivered by MetaCompliance has remained at 61. Most "All Staff" policies achieve around 94% awareness and agreement within three months of release. Whereas "Clinical" policies achieve around 92% awareness and agreement within the same timeframe.

The MetaCompliance system was replaced by a cloud based MyCompliance platform at the end of the year. The new platform continues to enforce selected policies, however the number of these has been reduced to lessen the impact of locking staff out of their PC's until they agree to

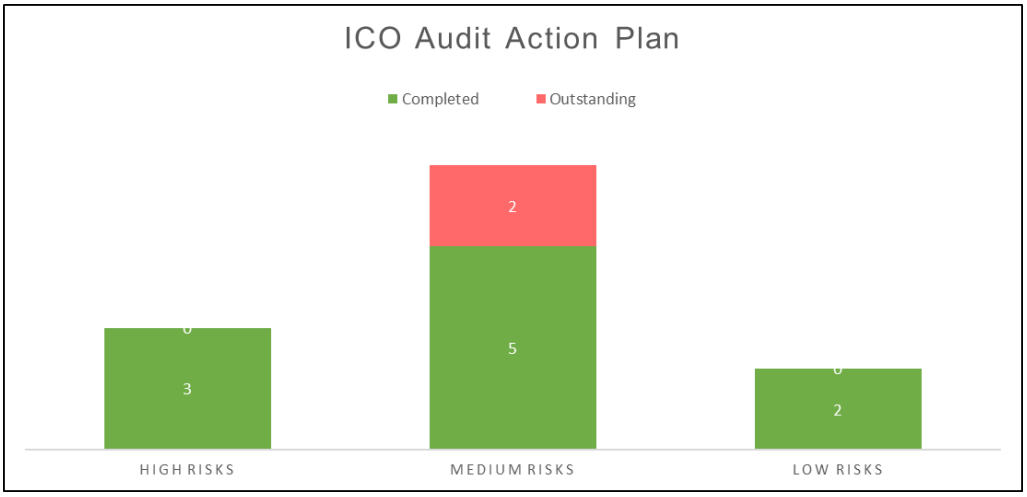
a policy. A self-service portal provides staff a convenient way to agree policies and quarterly management reports will start to be provided in the second quarter of 2024.

4 INFORMATION COMMISONER'S OFFICE AUDIT

The Information Commissioner's Office (ICO) audited the State Hospital to assess the risk of non-compliance with data protection legislation, the utilisation of ICO guidance and good practice notes and the effectiveness of data protection activities.

The audit was conducted in November 2022 with the organisation being awarded a high assurance rating.

The audit identified some areas were the state hospital could improve their compliance and following consultation with ICO a 12 point action plan was agreed to be completed over the next two years.



The organisation has now completed 83% of the action plan and only has two outstanding items. These relate to refresher training for Information Asset Owners and Information Asset Administrators as well as ensuring that there are resilience arrangements for their roles.

Training is planned in the second and third quarters of 2024/25.

5 IDENTIFIED ISSUES AND POTENTIAL SOLUTIONS

We have continued to try to improve attendance at the IGG meetings as full attendance at this group can sometimes be difficult to achieve – although continuing to have remote Teams meetings has encouraged a strong turnout. We encourage attendance by making the remit of the group relevant to staff members' roles, incorporating user feedback on eHealth matters into the agenda for the group. The attendance by deputies in the event of diary pressures is also now in place with a stronger emphasis for all members to encourage attendance.

Microsoft 365 (M365) implementation continues to be subject to a number of national delays. The groups tasked with delivering M365 have recruited more staff and it is hope that this will improve the speed of implementation nationally.

Staff who have duties that involve information governance tasks, such as subject access redaction should be suitably trained. A major training program will be delivered in 2024/25 to ensure that staff have appropriate training to support them in their roles.

Resourcing is always an issue, particularly when dealing with time limitations on statutory duties such as the supply of Subject Access Requests. Proposed solutions to assist in reducing the impact of this are being introduced, including the introduction of new software to assist with redaction and formal contingency plans with assistance from other departments if required.

6 FUTURE AREAS OF WORK AND POTENTIAL SERVICE DEVELOPMENTS

Work / Service Development	Timescale
Records Management Plan to be resubmitted	December 2024
Introduction of national Business Classification Schedule in shared drive areas	December 2024
Utilisation of software assisted redaction for subject access requests for clinical records	July 2024
Specialist Information Governance training program	April 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 2025