NHS 24
20 JUNE 2024
BOARD MEETING
ITEM NO 10.7
FOR ASSURANCE

INFORMATION GOVERNANCE AND SECURITY ANNUAL REPORT 2023/24

Executive Sponsor: Ann-Marie Gallacher, Chief Information Officer

Lead Officer/Author: Sanny Gibson, Head of Information Governance & Security & DPO

Action Required: The Information Governance and Security Annual Report 2023/23 is presented to the NHS 24 Board for assurance.

Key Points for this Committee to consider

The paper provides an overview of the key areas of activity for 2023/24 for the Information Governance and Security (IG&S) team in ensuring compliance with all legislative requirements. Included in the report are a number of key points;

- Completion through the year of all open ICO audit actions.
- The achievement of a LOW cyber exposure score rating.
- The improvement in the Network and Information Systems Regulations audit compliance [redacted]

Governance process

This paper was approved by the Information Governance and Security Group (IGSG) in April 2024. It was shared virtually with the Executive Management Team for awareness in April and was presented to the Planning and Performance Committee in May and Audit and Risk Committee in June. It is now presented to Board.

Strategic alignment and link to overarching NHS Scotland priorities and strategies

Effective Information Governance, Information Security and Records Management across NHS 24 supports delivery of NHS 24 services across the wider health and social care system.

Strategic alignment and link to Corporate Delivery Plan activity

The Corporate Delivery Plan has been submitted to Scottish Government and feedback is awaited.

Key Risks

This paper does not raise any new risks. It does, however, have a risk section which relates to risks contained on the Information and Cyber Security Risk Register. The

reporting and governance exercised by the Board Committees and the IGSG will have an impact on Information and Cyber risks.

Financial Implications
There are no direct financial implications arising from this report for 2023/24, though work reported here may result in the request for financial support in 2024/25.

Equality and Diversity
There have been no equality and diversity issues identified arising from this report.

1. RECOMMENDATION

1.1 The NHS 24 Board is asked to note Information Governance and Security Annual Report for the period 1 April 2023 to 31 March 2024. This report was presented to the Audit and Risk Committee meeting of 6 June 2024.

2. TIMING

2.1 This report sets out the activity of the Information Governance and Security team for 2023/24.

3. REPORT CONTENTS

3.1 The IG&S Annual Report for 2023-24 provides information on the following key areas including:

- Data Protection
- Freedom of Information & Environmental Information
- Information Security
- Policies Procedures and Protocols
- Records Management
- Data Protection Legislation
- Network and Information Systems Regulations
- Training
- Reportable Incidents
- Risk Management

3.2 The report details a number of audit and risk related items such as:

- The continuing volume of Data Subject Access Requests (DSARs) across the year. This was the highest number of requests received by NHS 24 in one year. While it has been a record year for DSARs the number received is still a very small percentage of the calls into NHS 24.
- The completion of all ICO audit actions through the year.
- The creation of a Cyber and Information Risk Register.
- The achievement of the target for the cyber exposure score, resulting in a rating of LOW exposure.
- The achievement of the Public Sector Cyber Resilience Framework (Scottish Government mandated framework) targets [redacted]

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications from this report, though it is expected that there will be financial implications from the 2024/25 work plans and for improvement works in relation to Data Protection and Security, both Information and Cyber.

INFORMATION GOVERNANCE AND SECURITY ANNUAL REPORT 2023/2024

BOARD MEETING

20 June 2024

Information Governance & Security Annual Report 2023/24

RECOMMENDATION

The Board is asked to note this report which provides assurance on the Information Governance and Security activity for the period 1 April 2023 to 31 March 2024.

BACKGROUND

The team continue to ensure the efficient and effective handling of information within NHS 24 in accordance with the following legislation and guidance frameworks:

- Data Protection Act 2018
- UK General Data Protection Regulation
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- Public Records (Scotland) Act 2011
- Access to Medical Records Act 1988
- Access to Health Records Act 1990
- Children and Young People (Scotland) Act 2014
- Computer Misuse Act 1990
- Digital Economy Act 2017
- The Network and Information Systems Regulations 2018
- Common Law Duty of Confidentiality
- Caldicott Principles (updated in December 2020)
- The Privacy and Electronic Communications Regulations 2003
- The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019

AREAS OF FOCUS

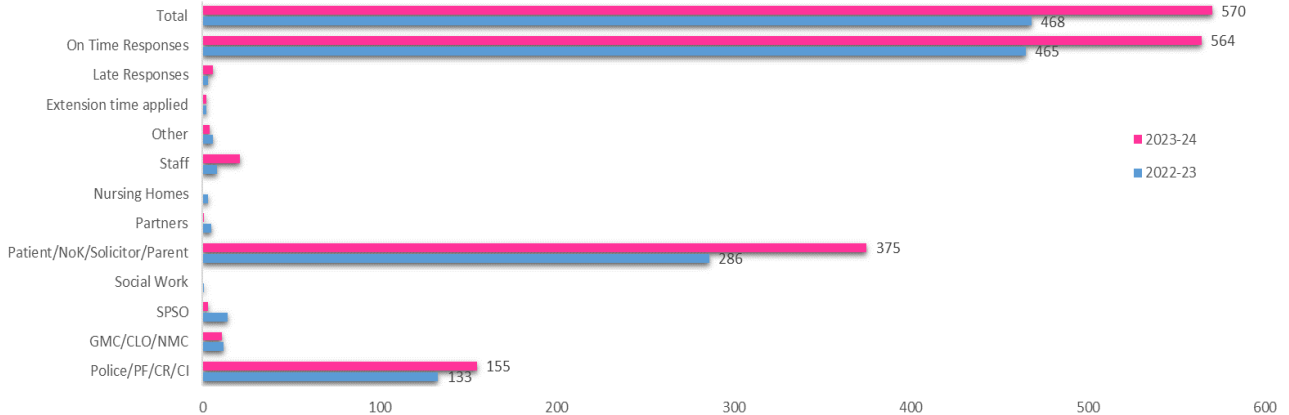
The Information Governance and Security Team focussed their work on a number of key areas during the period of this report:

- Data Protection
- Freedom of Information/Environmental Information
- Information Security
- Policies, Procedures and Protocols
- Records Management
- Data Protection Legislation
- Network and Information Systems Regulations
- Training
- Reportable Incidents
- Risk Management

Information Governance & Security Annual Report 2023/24

DATA PROTECTION

As a Data Controller pursuant to the Data Protection Act 2018 (DPA) NHS 24 is required to deal with Data Subject Access Requests (DSARs). These come from individuals who wish to know (and gain access to) their personal information held by NHS 24. Throughout 2023/24, NHS 24 received 570 requests, an increase of 22% on the levels processed during the previous year, 2022/23. The breakdown of applicants is shown below with 2022/23 as a comparison.



	Police/PF/CR/CI	GMC/CLO/NMC	SPSO	Social Work	Patient/NoK/Solicitor/Parent	Partners	Nursing Homes	Staff	Other	Extension time applied	Late Responses	On Time Responses	Total
2023-24	155	11	3	0	375	1	0	21	4	2	6	564	570
2022-23	133	12	14	1	286	5	3	8	6	2	3	465	468

The volume of requests received during 2023/24 was unprecedented and has far exceeded all previous reporting years. This increase has presented significant demands on the capacity of the Information Governance and Security team equating to 708.5 hours of processing time, the equivalent of approximately 19 working weeks (1 FTE). This does not include the time taken by colleagues across NHS 24 including Service Support Teams and Workforce.

Information Governance & Security Annual Report 2023/24

DATA PROTECTION (continued)

While the volume of data subject access requests have risen significantly in the last year, they represent only a fraction of the call volumes experienced by NHS 24. In 2023/24 there were 1,728,233 calls into the 111 service. The 549 DSARs, which were from all requesters except staff, equate to 0.03% of calls into the 111 service.

A technical system issue during the year delayed access to information requested on the six DSARs which were delivered late. All data subjects were kept fully informed during the period of the delay. To address the issue our managed service provider recommended a ‘work around’ that would ensure our ability to meet NHS 24's statutory obligations. This temporary solution however did not prove to be wholly successful. It was only through the perseverance of the team that a small proportion of responses were delayed. To ensure our requestors were aware of any potential delays, the team were proactive in providing progress updates, and complimentary feedback was received on our communications.

Requests come from a variety of sources. Those requests classified as *Others* were from; Disclosure Scotland; an MSP and two from The Royal College of Nursing.

The *Extension to Response Time applied* metric is for any requests which go outwith the preferred one calendar month deadline, and into a period of up to two further months (permitted under the legislation). There was one extension applied during Q1 of 2023/24 due to the complexity of the request. The request was responded to within the second extension month. The second request to have the extension time applied was because of the specific demands of the Applicant as to how they wanted the information provided to them.

DATA PROTECTION (continued)

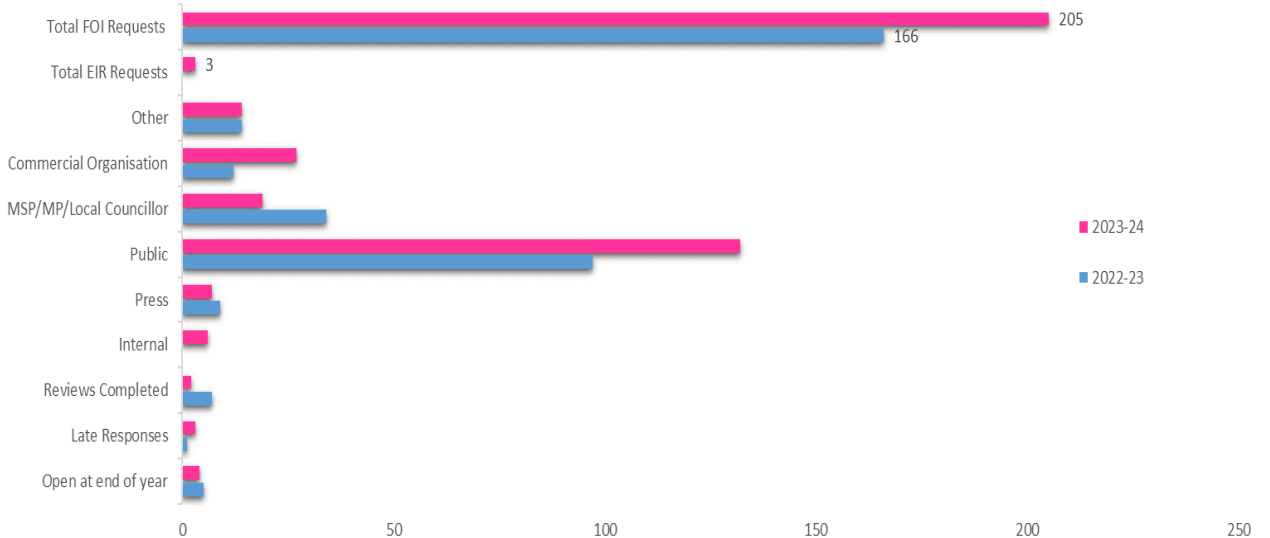
In 2023/24, Patient Experience received 310 complaints (across stage one and stage two). Of those, 17 were passed to IG&S to process as a Data Subject Access Request (these are included in the overall total of 570). This highlights again that sometimes requests do not always come through the intended route.

Amendments were applied to the NHS 24 websites to further the understanding of the public on the appropriate Health Board that they should submit a DSAR to. By providing this clarification, it is hoped that the positive impact is two-fold by reducing the impact on capacity in IG&S while assisting the public to gain access to their information sooner as they have a better understanding of who holds it.

Information Governance & Security Annual Report 2023/24

FREEDOM OF INFORMATION/ENVIRONMENTAL INFORMATION

The Information Governance and Security team coordinate responses to requests made under the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs). The number of requests for the year are shown below with 2022/23 as a comparison. Additional information regarding the FOI and EIR releases is provided below.

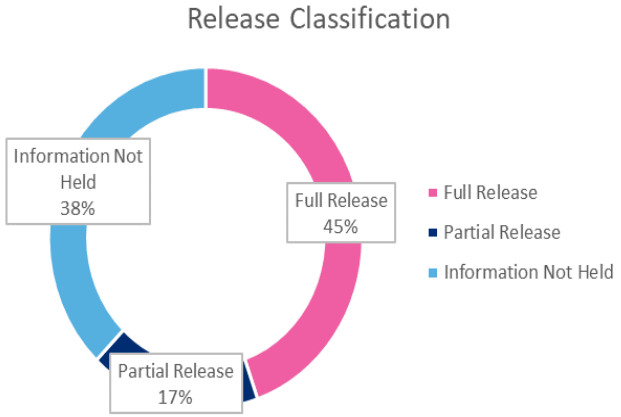


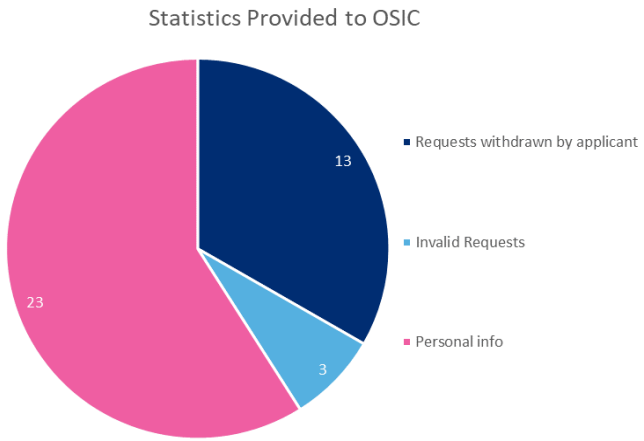
	Open at end of year	Late Responses	Reviews Completed	Internal	Press	Public	MSP/MP/Local Councillor	Commercial Organisation	Other	Total EIR Requests	Total FOI Requests
2023-24	4	3	2	6	7	132	19	27	14	3	205
2022-23	5	1	7	0	9	97	34	12	14	0	166

FREEDOM OF INFORMATION/ENVIRONMENTAL INFORMATION (continued)

During 2023/24 the level of FOI requests increased significantly, surging by 23.5% in comparison to 2022/23. This is a significant increase and has implications for the capacity of the team should levels increase further in the coming years. Based on trends over the last five years, the direction of travel indicates that further increases should be anticipated. As the requests can come from anyone anywhere in the world it is difficult to predict the number and nature of them.

A breakdown of the release classification of the requests and of the statistical information provided to the Scottish Information Commissioner is shown below:





FREEDOM OF INFORMATION/ENVIRONMENTAL INFORMATION (continued)

The IG&S team also deal with FOI requests which require an FOI review to be undertaken. This occurs when the requestor is not satisfied with the response provided. To ensure the integrity of our response, an FOI review panel is established comprised of FOI Leads that were not involved in the original response. Over the course of 2023/24 two such reviews of FOIs in relation to ICT contracts and Health Care issues were undertaken. The outcome of those reviews confirmed the accuracy and veracity of the original response collated.

On occasion individuals will mistakenly route their requests through incorrect channels. During the year this applied to 23 requests made under FOISA which were actually Data Subject Access requests.

This year the total number of hours spent, by the two Information Governance Officers (IGOs), on FOI Requests and FOI Reviews equated to just over 214 hours or approximately six working weeks (1 FTE). This does not include the time taken by the FOI Leads and colleagues within Communications to collate the information for the response.

The table below provides a breakdown of the time taken by the IGOs to process FOIs.

	FOI Requests	Time
Q1	48	52:29:00
Q2	57	68:39:00
Q3	40	41:22:00
Q4	60	51:37:00
Total	205	214:07:00

Information Governance & Security Annual Report 2023/24

INFORMATION SECURITY

Information Security focuses on three main principles, the confidentiality, integrity and availability of NHS 24 information. There is a requirement to ensure that these three principles are applied to the control of all NHS 24 information.

There have been several Information Security activities throughout the year as the Team strive to improve the information security and cyber security posture of the organisation.

NHS 24 utilise the [redacted] to measure the Exposure Score of Desktop and Laptop assets, [redacted]. The Exposure score rating [redacted]

The continuous cycle of software vulnerability disclosures and updates throughout the year caused a reduction in progress to the Exposure Score. However, a significant piece of work was undertaken in Q4 [redacted] coupled with aggressive asset housekeeping from BT, [redacted] Improvements have been made to the vulnerability management process which will help NHS 24 operate within its target operating range.

It is expected that further improvements will be made to the Exposure score after completing the implementation of [redacted] rules. These rules [redacted] include recommendations such as increasing the Windows Password length [redacted]

INFORMATION SECURITY (continued)

The above graph shows the cyber exposure score (lower is better) over 2023/24. [redacted] improvement activities in Q4 resulted in NHS 24 achieving a better than target score [redacted]

INFORMATION SECURITY (continued)

Several activities relating to improve Cyber Security Awareness were deployed throughout the year. These included the use of Team Talk and the in-Centre Wallboard displays to communicate important information relating to Reporting Phishing emails, Password Complexity rules and the promotion of policies such as the Clear Desk Clear Screen policy. Work will continue into 2024/25 with the Communications Team to further demonstrate NHS 24's commitment to Cyber Security Awareness.

Physical Security Reviews were conducted at South Queensferry and the new Aberdeen Site to provide reassurances to staff and look for opportunities to the improve the physical security of these sites. This activity will continue in 2024/25 in conjunction with the Scottish Ambulance Service.

As such, appropriate access controls are progressing with Aberdeen site Landlords with a view to completing commissioning in Q1 2024/2025. Furthermore, a procurement exercise to replace Legacy CCTV and door access hardware at Norseman House, South Queensferry was successful, work is underway and will be completed Early Q1 2024/2025 providing significant improvements to CCTV coverage.

Members of ICT and other directorates participated in a Cyber Desktop Exercise, simulating NHS 24's response to a Ransomware Incident. [redacted] the next planned Cyber Incident Desktop Exercise [redacted].

POLICIES, PROCEDURES & PROTOCOLS

A number of policies and processes covering Data Protection, Information Security, Records Management and Freedom of Information have been reviewed, updated and approved throughout the course of the year. All have undergone due diligence by the Information Governance and Security Group prior to approval.

- Appropriate Policy Document
- Archive and Transfer Policy
- Clear Desk Clear Screen Policy
- Cryptography Policy
- Data Protection Impact Assessment Policy
- Data Protection Notice (Easy Read Version)
- Data Protection Notice (Arabic)
- Data Protection Notice (Kurdish Sorani)
- Data Protection Notice (Polish)
- Data Protection Notice (Romanian)
- Data Protection Notice (Simplified Chinese)
- Data Protection Notice (Spanish)
- Data Protection Notice (Ukrainian)
- Document Version Control & Naming Convention Standards

POLICIES, PROCEDURES & PROTOCOLS (continued)

- IGSG Terms of Reference
- Information Security Incident Management Policy
- Password Management Guidelines
- Password Management Policy
- Records Retention and Destruction Policy
- Records Retention Schedule
- Remote Access Policy
- Removable Media Policy
- Staff Data Protection Notice
- Subject Access Request Process
- Vulnerability Management Policy

RECORDS MANAGEMENT

During 2023/24 the IG&S team have continued to ensure NHS 24 maintains robust practices in relation to our statutory obligations on Records Management.

Internally we have:

- Undertaken an annual review of the Records Management Policy;
- Developed a Records Management eLearning module in collaboration with our colleagues in Organisational Development Leadership and Learning (ODL&L). This will be released to the wider organisation via TURAS during 2024/25;
- Reviewed the off-site storage contract with the supplier Restore in conjunction with Procurement, Finance and ICT colleagues. This has resulted in the contract being reworked to better reflect the needs of NHS 24;
- Continued to work with Directorates as part of the quarterly Directorate Information Asset Review on reviewing their information assets, record of processing activities, documents stored in off-site storage, items that are suitable for permanent preservation with National Records of Scotland (NRS), the status of their Data Protection Impact assessments (DPIAs) and any data sharing/ processing agreements; and
- Commenced evidence collation and improvement works in line with the voluntary Progress Update Review (PUR) that National Records of Scotland (NRS) has invited us to participate in. It is anticipated that this will be completed during 2024/25 prior to the development of a new five-year Records Management Plan for NHS 24.

RECORDS MANAGEMENT (continued)

The IG&S team recognise the importance of maintaining strong working relationships with other NHS boards, Scottish Government and NRS. This is key to informing our records management strategy and practice as we move forward. During 2023/24 we have:

- Regularly attended the quarterly NRS surgeries and NHS-wide forums to build networks, benefit from learning and sharing good practice;
- Participated in a national review of the Scottish Government Records Management Code of Practice for Health and Social Care 2020 and provided feedback on areas of development;
- Participated in a short life working group (SLWG) focusing on Digitisation and Digitalisation of records feeding into the revision of the Scottish Government Records Management Code of Practice for Health and Social Care 2020. The SLWG will feed into the Records Management Code of practice delivery group overseen by the Scottish Government National Information Governance Programme Board;
- Met with the off-site storage account manager and recommended improvements to the user access portal. These improvements will ease the retrieval of redundant information and increase the accuracy of the records held; and
- Assisted NRS with the development and testing of their Public Sector Storage survey.

DATA PROTECTION LEGISLATION (INCLUDING UK GDPR)

NHS 24 have statutory obligations around the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR).

Throughout the year the Data Protection (Privacy) Notice which is published on the web sites was updated to reflect changes that had been identified as part of various Data Protection Impact Assessments (DPIAs). DPIAs are required (Article 35 of the UK GDPR) where processing of personal data or special categories of personal data may result in a high risk to the rights and freedoms of natural persons. Using the DPIA process is a way to assess the risks and identify any mitigations to reduce that risk to a level that can be accepted by NHS 24.

During 2023/24 the following DPIAs were supported by the IG&S team and subsequently reviewed by the DPIA Panel, Data Protection Officer, Information Asset Owner (IAO) and Senior Information Risk Owner (SIRO):

- National CHI
- Scottish Emergency Dental Service Childsmile
- Scottish Ambulance Service Warm Transfer to NHS 24 Mental Health Hub
- NHS 24 data transfer of contact information to Scottish Ambulance Service
- Redesigned Urgent Care (RUC) Pathway Evaluation
- Verint Voice Analytics
- Forensic Medical Services
- Hotjar - user engagement tool
- Pushfar – staff mentoring
- Amiqus – onboarding identity check platform
- WFM – workforce management module
- AON – online assessments

DATA PROTECTION LEGISLATION (INCLUDING UK GDPR) (continued)

Continuous improvement is a key priority for the IG&S team. Consequently, actions arising from the ICO Audit which was undertaken during Q4, 2022/23 were concluded during 2023/24. These include:

Recommendations

1) Update Data Processing Agreement (DPA) Register – LOW - **Complete**.

2) Review of compliance of existing DPAs on register – LOW - **Complete**.

3) Easy Read translation of the Data Protection Notice – MEDIUM - **Complete**.

4) Project Initiation Document and Procurement Handbook to include DPIA section LOW – **Complete**.

5) Review of Hard copy DPIA register LOW – **Complete**.

6) Breach Reporting Guidance – schedule to be delivered in Q4 LOW – **Complete.**

DATA PROTECTION LEGISLATION (INCLUDING UK GDPR) (continued)

The IG&S team undertook a review of the current DPIA process in January 2024. The outcome of the review highlighted that while, colleagues have a strong grasp of the importance of data protection, there were areas which would benefit from awareness raising activities. To this end, the team have collaborated with Communications to produce new wallboards in NHS 24 offices as friendly reminders for staff of what constitutes personal and special category data.

To compliment the wallboards, the IG&S team have developed two seven-minute briefings on the UK GDPR principles and the importance of undertaking Data Protection Impact Assessments (DPIAs) at the start of any project or business change. Feedback has been positive and is informing the IG&S team as they develop bespoke training sessions for delivery across NHS 24 teams throughout 2024/25.

NETWORK AND INFORMATION SYSTEMS REGULATIONS

As an Operator of Essential Services (OES) NHS 24 are subject to the UK implementation of the Security of Network and Information Systems Directive which is the Network and Information Systems Regulations 2018 (NIS-R).

In July 2023, NHS 24 was audited against the Public Sector Cyber Resilience Framework (PSCRF), measured by the Health Competent Authority using these Key Performance Indicators (KPIs):

- Overall Compliance should be at ≥ 60% ([redacted])
- 60% of Categories should have a compliance of ≥ 60% ([redacted])
- There should be zero subcategories with a compliance of <30% ([redacted]).

[redacted] have now been self-assessed as compliant, in line with the auditing process and will be formally assessed at the next review audit in July 2024.

The NHS 24 ICT audit plan has been updated to track progress of the NIS-R 2024 and 2025 review audits. Work is actively underway on improved compliance against the controls determined by the auditors as not being fully compliant for the 2024 review audit. This work involves staff across NHS 24 as the controls within the PSCRF are across the entire organisation and with NHS 24's managed service provider where there is an opportunity to make improvements on controls within their remit.

TRAINING

Training and awareness for information security, data protection, freedom of information and records management are essential in any organisation subject to the relevant legislation for those disciplines.

All ICO reportable breaches are required to confirm the training status, over the last two years, of any staff involved in the breach.

There are three eLearning modules currently available for staff, with two of those modules (Safe Information Handling (Data Protection) and Stay Safe Online (Information Security) being categorised as statutory requirements. The Freedom of Information module is not yet categorised as statutory; this will be reviewed with the ODL&L Team in 2024/25 for consideration. The Records Management module will be released in 2024/25.

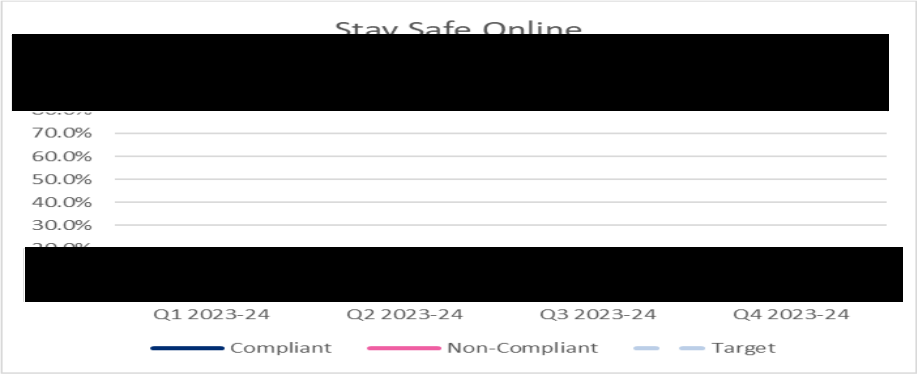
Approval was given by the Executive Management Team to expand the Cyber Security training and awareness capability which is an audit improvement recommendation. This was procured in Q4 and implementation will be taken forward in 2024/25 with the ODL&L Team.

The IG&S team have also delivered in-person induction and on demand training across NHS 24 throughout the year and have helped raise awareness through regular content in Team Talk and the previously noted in-centre wallboards and seven-minute briefings.

Throughout the year the IG&S team have been reporting the directorate and overall compliance figures and working with both the ODL&L team and the IAOs on progress towards the 95% overall compliance target.

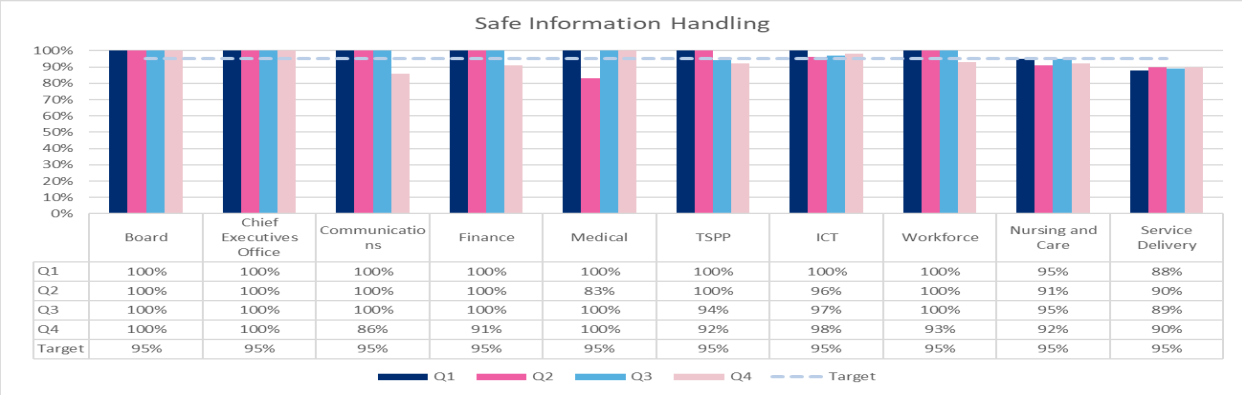
TRAINING (continued)

The compliance status for the Safe Information Handling (SIH) and the Stay Safe Online (SSO) eLearning packages are displayed below. These graphs evidence training levels throughout the year, which are reflective of staffing changes. While levels are consistently high, the 95% overall target, while close, has not yet been achieved. [redacted]

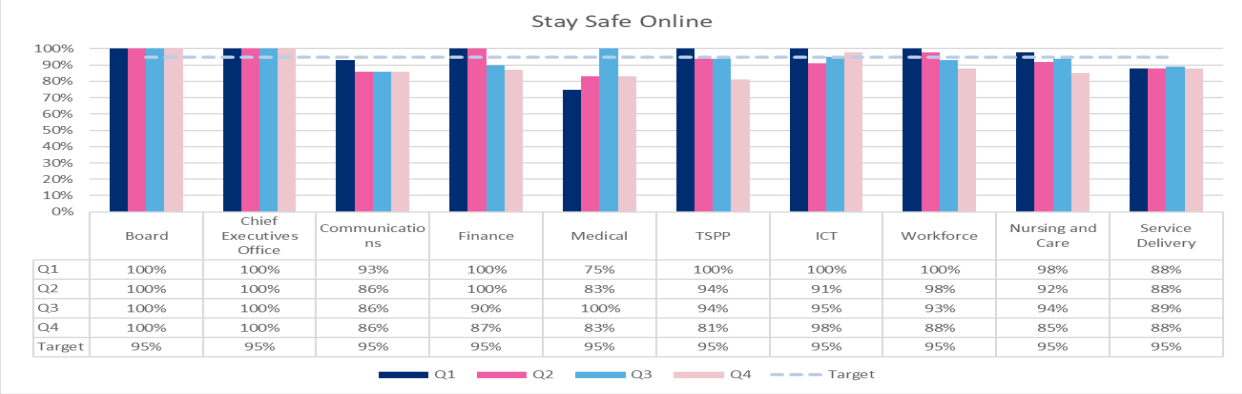


TRAINING (continued)

All Directorates have been consistently high in completion status for both statutory eLearning modules with a number having achieved 100% compliance. Service Delivery (as the largest directorate) continue with a high uptake typically holding around 90% compliance.



	Board	Chief Executives Office	Communications	Finance	Medical	TSPP	ICT	Workforce	Nursing and Care	Service Delivery
Q1	100%	100%	100%	100%	100%	100%	100%	100%	95%	88%
Q2	100%	100%	100%	100%	83%	100%	96%	100%	91%	90%
Q3	100%	100%	100%	100%	100%	94%	97%	100%	95%	89%
Q4	100%	100%	86%	91%	100%	92%	98%	93%	92%	90%
Target	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%



	Board	Chief Executives Office	Communications	Finance	Medical	TSPP	ICT	Workforce	Nursing and Care	Service Delivery
Q1	100%	100%	93%	100%	75%	100%	100%	100%	98%	88%
Q2	100%	100%	86%	100%	83%	94%	91%	98%	92%	88%
Q3	100%	100%	86%	90%	100%	94%	95%	93%	94%	89%
Q4	100%	100%	86%	87%	83%	81%	98%	88%	85%	88%
Target	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%

REPORTABLE INCIDENTS

As part of the regulatory regime that NHS 24 operates within, an incident which has resulted in a breach of either the Data Protection Legislation or the NIS Regulations (NIS-R) must be considered and assessed against certain criteria. If the incident is considered to have met the criteria, then it must be reported to the relevant regulator or, if appropriate, to both regulators.

In the period of this annual report, 20 incidents were investigated by the Information Governance & Security Team, of which 2 were reported to the Health Competent Authority as a breach of NIS Regulations, and 1 was reported to the Information Commissioners Office.

Both NIS-R instances related to the loss of availability in the NHS 24 111 Unscheduled care service. The first was due to [redacted] issue impacting Sinch Contact Centre, and the second was due to a UK wide issue in the Vodafone 111 platform.

The ICO reportable incident related to an investigation into an artefact which was found on a printer where the sender had an expectation of confidentiality relating to the contents of the printed email.

All reported incidents were closed with no follow up action required from the regulators.

RISK MANAGEMENT

Information Security and Governance are risk management exercises. The IG&S team regularly review existing and propose new risks. Where it is appropriate the team take ownership for the mitigation of these risks or work with the appropriate owners to consider and implement appropriate risk mitigations.

Through 2023/24 the IG&S team, in conjunction with relevant staff from other departments developed, and had approved, a set of Key Risk Indicators (KRIs). These indicators are used in conjunction with a list of cyber threats. This information is used to populate and assess cyber threats to NHS 24.

This resulted in the development of a Cyber Security Risk Register which details a number of Cyber Risks to NHS 24. The risks on this register were reviewed through the year with mitigating actions implemented to reduce the risks to a point where they are retained and then monitored.

This monitoring of retained risks is important as cyber risks are subject to change and the risk score and status amended based on the KRIs and cyber threat intelligence gathered from sources such as the National Cyber Security Centres *Connect Inform Share Protect* (CISP) platform which is a secure and confidential information sharing and collaboration environment.

One overarching Cyber Security Risk was entered on the Corporate Risk register.

In the latter part of the year a review of information governance risk was undertaken, these will be added to the Information and Cyber Risk Register in 2024/25 and this joint register will be reviewed and managed throughout the year.

RISK MANAGEMENT (continued)

A report on the status of the risks on the Information and Cyber Risk register will be presented to the Information Governance and Security Group at the quarterly meetings.

At the time of this report there are fourteen open risks on the Information and Cyber Risk Register with seven of those set to Retain for monitoring. The remaining risks have current mitigating actions in place to reduce the assessed score.

There are seventeen Information risks proposed for the register which are under review prior to official entry to the register. The information risks use the information triad established under the UK GDPR and Data Protection Act 2018 of Confidentiality Integrity and Availability (CIA).

Of the seventeen proposed seven would be entered on the register as monitoring or retained risks which would allow them to be reviewed as part of the monitor/retain risk process.

FINANCIAL IMPLICATIONS

There are no direct financial implications from this report, though it is expected that there will be financial implications from the 2024/25 work plans and for improvement works in relation to Data Protection and NIS-R legislation and physical security improvements.