NHS 24
BOARD MEETING

22 JUNE 2023
ITEM NO 10.3
FOR APPROVAL

INFORMATION GOVERNANCE AND SECURITY ANNUAL REPORT 2022/23

Executive Sponsor:	Chief Information Officer, Ann-Marie Gallacher
Lead Officer/Author:	Head of Information Governance & Security & DPO, Sanny Gibson
Action Required	This report is presented to the Board for their approval.
Key Points for the Committee	The paper provides an overview of the key areas of activity for 2022/23 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; • The marked improvement in the cyber exposure score after completion of the Connect Programme and the associated Early Life Support Period. • The volume of Data Subject Access Requests remains at a very high level for the second year. • The completion of the process to have National Records of Scotland confirmed as the official Archivist for NHS 24. • The positive trend throughout the year in the completion of the Information Governance and Information Security training, which is a statutory requirement, with both modules exceeding 90% compliance.
Governance Process	The Information Governance and Security Group (IGSG) approved the report in April 2023. The Executive Management Team and the Planning and Performance Committee received the report in May 2023 and the Audit and Risk Committee in June 2023 for Assurance and it is now presented to the Board for Approval.
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.
Key Risks	This paper does not report directly on specific risks, however the reporting and governance exercised by the Board Committees and the IGSG will have an impact on IG&S risks.
Financial Implications	There are no direct financial implications arising from this report for the year 2022/23, though work reported here may result in the request for financial support.

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

1. RECOMMENDATION

1.1 The Board are asked to approve this report which provides assurance on the Information Governance and Security activity for the period 1 April 2022 to 31 March 2023.

2. TIMING

2.1 This report sets out the activity of the Information Governance and Security team for 2022/23 for approval at the Board Meeting in June 2023.

3. REPORT CONTENTS

3.1 The IG&S Annual Report for 2022/23 provides information on a number of key areas including:

- Data Protection Act
- Freedom of Information & Environmental Information
- Information Security
- Policies Procedures and Protocols
- Records Management
- Data Protection Legislation (Including UK GDPR)
- Network and Information Systems Regulations
- Training
- Reportable Incidents
- Risk Management

3.2 The report continues with the new style first used in the Q3 report.

3.3 The report details a number of planning and performance and risk related items such as:

- The continuing volume of Data Subject Access Requests across the year, while still high are a fraction of the call volumes into NHS 24.
- The closure of a number of risks across the year.
- Improvements throughout the year in the compliance for both data protection and information security training with the continuing uptake of the Stay Safe Online and Safe Information Handling eLearning modules.
- Improvements in the overall compliance against the Network and Information Systems Regulations review which completed the initial three-year audit cycle (the new three-year cycle starts in 2023).
- The reduction in the cyber exposure score over the final quarter of 2022/23 after completion of Connect Phase 1 and the associated Early Life Support Period.

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 2023/24 work plans and for improvement

works in relation to Data Protection and NIS-R legislation and physical security improvements.

INFORMATION GOVERNANCE AND SECURITY ANNUAL REPORT 2022 / 2023

BOARD MEETING

22 June 2023

Information Governance & Security Annual Report 2022/23

RECOMMENDATION

The Board is asked to approve this report which provides assurance on the Information Governance and Security activity for the period 1 April 2022 to 31 March 2023.

BACKGROUND

The team continue to work conscientiously to ensure handling of information within NHS 24 is done 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

Information Governance & Security Annual Report 2022/23

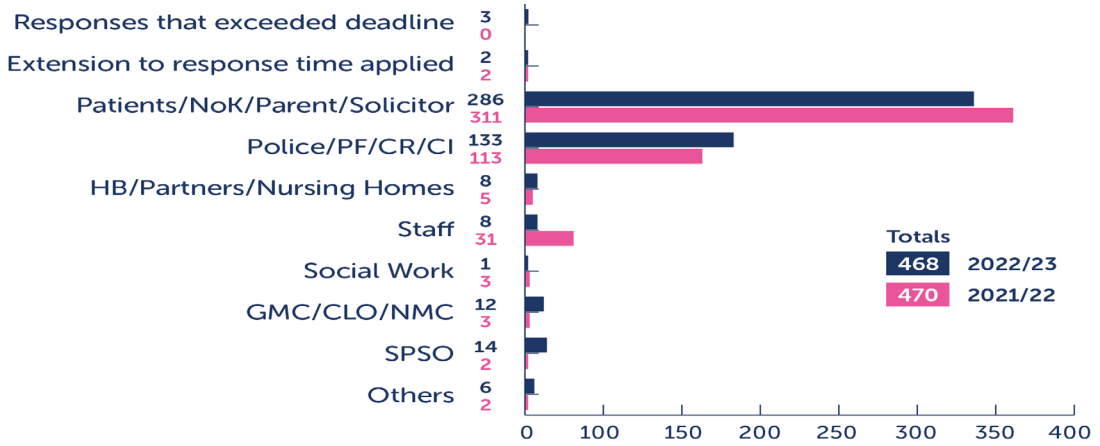
AREAS OF FOCUS

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 (Including UK GDPR)
- Network and Information Systems Regulations
- Training
- Reportable Incidents
- Risk Management

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) from individuals who wish to know (and gain access to) the personal information that NHS 24 holds on them. Throughout 2022/23 NHS 24 dealt with 468 requests. The breakdown of applicants is shown below with 2021/22 as a comparison.



As can be seen from the graph this has been (though with two fewer requests than 2021/22) another very busy year for DSARs. Dealing with this volume of requests is challenging because the number of requests do not directly relate to the effort involved as most requests are multi-part.

*The Responses exceeded and Extension to Response are counted in the relevant *Sources* figures e.g. *Parents/NoK etc.*

DATA PROTECTION (continued)

While the volume of requests remains high it is still only a fraction of the call volumes experienced by NHS 24. In 2022/23 there were 1,919,537 calls into the 111 service, which means that the DSAR requests were 0.02% of the 111 call volumes.

A technical issue during the year delayed access to the information requested on a number of DSARs. The resolution required a multi-party response. While it was a live issue the managed service provider recommended a work around. This had a very intermittent success rate. The perseverance of the team minimised the number of delayed responses, though it could not eradicate them. Regular communication with the applicants kept them apprised of progress which was appreciated by the applicants.

The requests classified as *Others* were from; MSPs on behalf of constituents (two); private health insurance companies in relation to claims (two); Angelia Research seeking information on behalf of a family and the Scottish Social Services Council in relation to an investigation.

The *Extension to Response Time applied* metric is for any requests which go outwith the preferred one calendar month deadline for a response into a period of up to two further months (permitted under the legislation). The extensions applied through this year were both in Q2 and were because of their complex nature as the requests were linked and were both DSAR and Rectification requests. The requests were responded to within the second extension month.

DATA PROTECTION (continued)

In 2022/23, IG&S responded to a similar number of Data Subject Access Requests (468) compared with the number of complaints received by NHS 24 (439). While they were of a similar number, only 13 of the complaints received by Patient Experience were passed to IG&S for a data subject access request element.

Changes were made to the NHS 24 websites to further the understanding of the public on the appropriate Health Board that they should submit a DSAR to. This helps to reduce the burden on IG&S and helps the public get access to their information sooner as they have a better understanding of who holds it.

FREEDOM OF INFORMATION & ENVIRONMENTAL INFORMATION

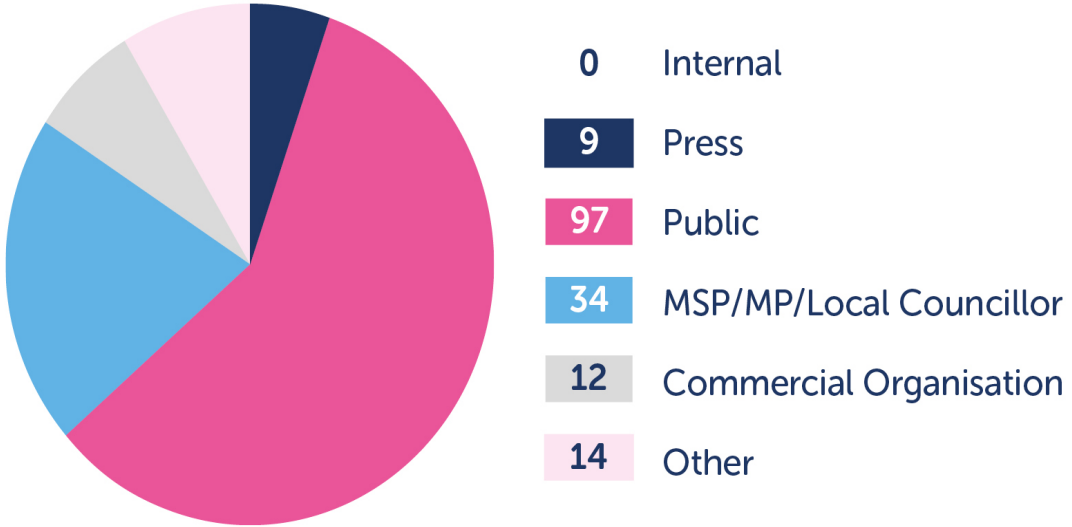
The Information Governance and Security Team coordinate requests for information under the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs). The number of requests for the year are shown below with 2021/22 as a comparison. Additional information regarding the FOI and EIR releases is provided below.

	2022-23	2021-22
No. of FOI requests received	166	330
No. of EIR requests received	0	2
No. of FOI reviews completed	7	1
Number of responses Issued:		
On time	160	320
Late	1	2
Full Release	71	49
Partial Release	17	28
Information not held	31	126
Still open at year end	5	10
Statistics reported to the SIC		
No. of requests closed because of no clarification	2	3
No of requests withdrawn by Applicant	5	41
Invalid requests	5	24
Repeat requests	1	2
Personal Information	20	37
Refusal Due to Cost	0	0
Otherwise Accessible	7	20
Intended for Future Publication	2	2

FREEDOM OF INFORMATION & ENVIRONMENTAL INFORMATION (continued)

There was an almost 50% decrease in FOISA requests in comparison to 2021/22. As the requests can come from anyone anywhere in the world it is difficult to predict the number and nature of them.

The majority of the requests were received from members of the public; a breakdown of the valid request sources is shown below:



FREEDOM OF INFORMATION & ENVIRONMENTAL INFORMATION (continued)

The seven reviews listed in the table were in relation to ICT contracts (x3), 111 calls (x2), and Equality and Diversity (x2). In the seven, the Review Panel responses were as follows:

- 3 were confirmed without modification to the original response;
- 1 was modified with additional information being provided in an Excel workbook;
- 1 was modified with a mistyped/incorrect email address being corrected;
- 1 was modified after clarification on any advice provided by Scottish Government
- 1 is currently still open at the time of this report.

Twenty of the requests received through the year were actually DSAR requests which were submitted by the applicants as FOI requests. A temporary change to the reporting meant these were not included as FOI requests from Q1 to Q3. That temporary change has now been lifted and these requests, which are classed as FOISA Section 38 requests, are now included in the annual table. They have to be responded to as both FOI and DSAR requests.

Two requests were responded to as Section 27 requests where the information requested will be published by the organisation at a date not later than 12 weeks after the requests were received. NHS 24 are required to have a publication scheme and consideration will be given to what additional information could be published which may help reduce the number of FOI requests.

There was one late response which was in Q4, the applicant was satisfied with the slight delay.

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 a number of Information Security activities throughout the year as the Team strive to improve the information security and cyber security posture of the organisation.

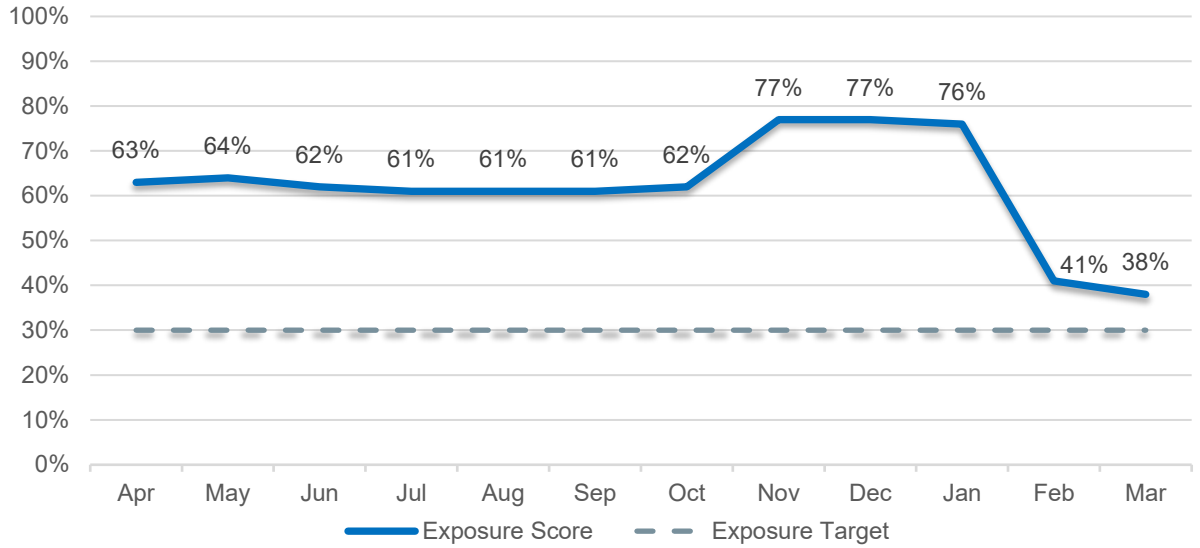
A number of the initiatives were incorporated into elements of the Connect programme. Following the conclusion of 1C of the programme and its associated Early Life Support (ELS) period, regular patching has recommenced and has made a significant improvement to the Defender for Endpoint Exposure score (this is a measure of the cyber security posture where NHS 24 have set a target of 30 and below).

That follows on from the migration to Windows 10 and the associated upgrade to version 21H2 which allows for full patch deployment.

Footprint reduction (removal of software) of Google Chrome and Java has also had a positive impact which is reflected in the reduction in Exposure score.

The implementation of the 14-day patching life cycle as a significant improvement has also been a major mitigation in a number of security risks.

INFORMATION SECURITY (continued)



The above graph shows the cyber exposure score (lower is better) over 2022/23 with the implementation of the improvement activities following the Winter change freeze and the Festive period. While still above the target of 30% there has been significant improvement on the reduction of the exposure which will continue through 2023/24.

INFORMATION SECURITY (continued)

Other cyber related improvements implemented through the year include mitigation against denial of service attacks and implementation of threat intelligence feeds which help protect against threats to certain public facing elements of the estate.

Changes in NHS 24's physical estate such as the closure of Kings Cross and Orkney, along with the expansion at Lumina, has driven necessary changes in CCTV, Access Control and Physical Security Assessments.

The team have continued, throughout the year, to improve staff knowledge on both information governance and information security with regular articles being delivered through the TeamTalk communications channel.

Programme support has also included penetration testing and remediation and an external security review of the standard desktop and laptop builds.

While there was penetration testing and remediation done as part of the Connect programme that testing was not (as determined by an internal audit) deemed as being a full estate-wide test. That, along with other recommendations, was provided as output from the internal audit on Cyber Resilience and Recovery which was delivered in Q4.

The implementation of those recommendations will form part of the basis of improvement works which will also provide evidence for the new three year audit cycle of the Security of Network Information System Regulation 2018 which will take place in Q2 2023/24.

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.

- Call Download Process V2.0
- Clear Desk Clear Screen Policy V3.0
- Cyber Security Risk Management Policy V2.0
- Data Cleanse Policy V3.0
- Data Protection and Confidentiality Policy V5.0
- Data Protection Impact Assessment Policy V2.0
- Data Protection Impact Assessment Procedure V1.0
- Email Acceptable Use Policy V1.0
- Information Classification Scheme Policy V3.0
- Information Governance Policy Statement V2.0
- Information Governance & Security Policy on Policies V1.0
- Information Governance & Security Training Strategy V1.0
- Information Security Incident Management Policy V4.0
- Information Security Policy V4.0
- Information Security Policy Statement V5.0
- Information Security Risk Management Policy V2.0
- Internet Acceptable Use Policy V2.0

POLICIES, PROCEDURES & PROTOCOLS (continued)

- Malicious Software Protection Policy V3.0
- Mobile Device Management Policy V1.0
- Multiple Records Management Process V3.0
- Physical Security Policy V3.0
- Records Management Policy V3.0
- Records Retention and Destruction Policy V4.0

RECORDS MANAGEMENT

After a hiatus through the Covid restrictions the Records Management Group (RMG) was reconvened during 2022-2023. This group brings focus across all directorates to records management which underpins legislation such as FOISA and the DPA.

The National Records of Scotland (NRS) Deposit Agreement – which allows NHS 24 to use NRS as the official archivist for the organisation – was completed and signed by NHS 24 and NRS. This was a first for NHS 24 in having an official archivist and archive capability for records which are designated for archive in the Scottish Government Records Management: Health and Social Care Code of Practice (Scotland) 2020 and the NHS 24 Records Retention Schedule. This will allow the transfer of records that are appropriate for archive.

NHS 24 submitted a Progress Update Report (PUR) to NRS in Q1. This is evidence which allows for an assessment by NRS of the implementation of NHS 24's Records Management Plan. The initial draft report was reviewed and after feedback from IG&S the final report was published by NRS in December 2022. The report is available via the attached link:

https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/NRS_PRSA_NHS_24_Progress_Update_Review_%28PUR%29_2021_Final_Report_Web_Version_02_December_2022.pdf

RECORDS MANAGEMENT (continued)

The IG&S team have also reviewed the off-site storage contract which is in place with the supplier Restore. This was done in conjunction with Procurement, Finance and ICT colleagues. Work continues, as part of the quarterly Directorate information asset review, on the information stored in the off-site storage facility.

The IG&S team in conjunction with the Information Asset Administrators (IAAs) and Organisational Development Leadership and Learning (ODL&L) colleagues have developed a Records Management eLearning module. The module has been reviewed by the IG&S team and, subject to minor changes, will be shared with the records management group for comment.

During the period of the report the IG&S team have participated in a national review of the Scottish Government Records Management: Health and Social Care Code of Practice (Scotland) 2020 and provided feedback on areas of development.

Also during the period of the report the IG&S team have 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: Health and Social Care Code of Practice (Scotland) 2020. The SLWG will feed into the Records Management Code of practice delivery group overseen by the Scottish Government National Information Governance Programme Board.

DATA PROTECTION LEGISLATION (INCLUDING UK GDPR)

NHS 24 are required to comply with relevant data protection legislation, such as the Data Protection Act 2018 and the UK General Data Protection Regulations.

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 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.

Through this year a number of DPIAs were progressed and then passed for approval to the relevant Information Asset Owners (IAOs) and the Senior Information Risk Owner. These included:

- Mental Health Police Scotland (Mental Health Collaboration Phase 2)
- Connect 1C (Reporting Stack)
- Connect 1C (Clinical Stack)
- Self-Referral Telephony Service and NHSinform content for Forensic Medical Examinations
- Mind to Mind

DATA PROTECTION LEGISLATION (INCLUDING UK GDPR) (continued)

- Surviving Suicidal Thoughts
- Audio Recordings for the Enhanced Practitioner Programme
- NHS 24 Mobile App

The DPIA process has been refined through the year with the assistance of the members of the DPIA Panel who come from across the organisation. Part of this refinement is the migration to the electronic system and the development of the DPIA workflow within that system. This will allow for better reporting of DPIA status and automatic review reminders.

A major programme under the DP legislation was the audit by the UK regulator, the Information Commissioner's Office (ICO). The ICO are undertaking this audit programme across all NHS Scotland Boards.

NHS 24 undertook the audit in Q4, this involved providing documentation and evidence to the ICO, prior to a series of interviews with a number of NHS 24 staff which took place over three days in March.

The NHS 24 response to the ICO draft report required additional evidence and representation from NHS 24. In the audit process over 160 items of documentation and evidence were provided. The final ICO assessment and report will be delivered very early in Q1 2024.

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 Security of Network and Information Systems Regulations 2018 (NIS-R).

The Scottish Government, as the Health Competent Authority (HCA), had implemented a three year audit cycle which started in 2020. The audit scope was the Security Policy Framework which was implemented across the NHS. NHS 24 completed the final review of that three year cycle in August 2022 and the report was received in October 2022.

Overall compliance from the 2020 report, through the 2021 and 2022 reviews has increased from 33%, to 46% and 51% respectively.

In May 2022 the HCA announced a plan to introduce Key Performance Indicators (KPIs) as part of the new audit cycle. The initial target for introduction of this KPI in December 2023 will see the Boards being measured against a published target KPI (referred to as the 60-60-0 KPI). That KPI is broken down as follows:

- Overall Compliance should be at ≥ 60%
- 60% of Categories should have a compliance of ≥ 60%
- There should be zero subcategories with a compliance of <30%

NETWORK AND INFORMATION SYSTEMS REGULATIONS (continued)

The 2022 final review report translates to the following representation of the KPIs:

- Overall compliance – 51%
- 37% of subcategories have a compliance of ≥ 60%
- 16 subcategories with a compliance of <30%

The 2022 review was the last undertaken against the NHS Scotland Security Policy Framework. The NIS-R audit schedule will recommence in 2023/24 and the Boards will be audited against the Scottish Government Public Sector Cyber Resilience Framework (CRF). This means that all public sector bodies (including NHS Scotland Boards) will be audited against the same set of controls, where previously different standards and controls were being utilised.

NHS 24 will be audited in Q2 2023/24 against the revised Cyber Resilience Framework with evidence to be submitted to the regulator by mid-July and the on-site element taking place in August.

TRAINING

Mandatory training across the organisation has been a focus for all Directorates. During the course of the year the IG&S Team were involved in a Short Life Working Group (SWLG) which reviewed all mandatory training.

As part of that SLWG the Information Governance and Security training was designated as Statutory. This change in designation identifies the Information Governance and Security training packages as a regulatory requirement and not just NHS 24 mandated training packages.

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

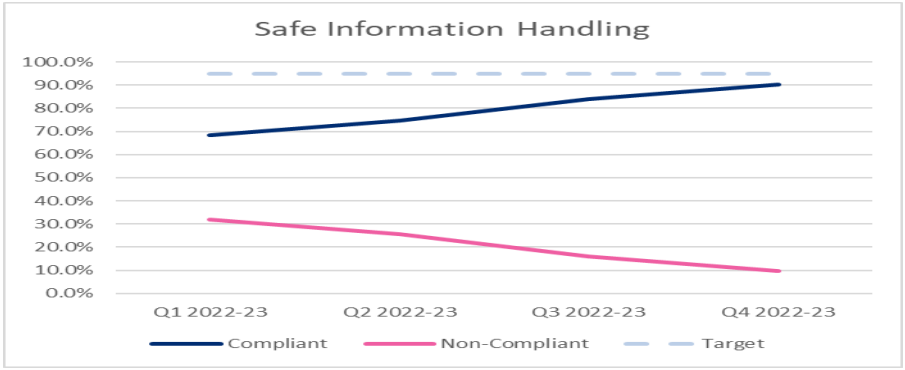
Throughout the year the IG&S team have been reporting the directorate and overall compliance figures and working with both the ODL&L team and the IAOs on progress towards the 95% overall compliance target.

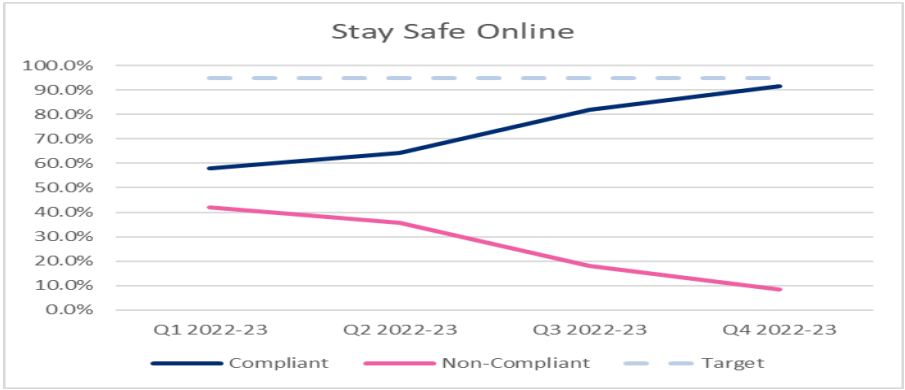
Training has also been delivered, procured and attended. One member of the Team attended and achieved Freedom of Information Practitioner status. External training was procured for the IAOs and IAAs on data protection with a follow up briefing to the IAOs on data processing and data sharing agreements.

The Team delivered data processing and data sharing agreement training to SAS Procurement as they provide procurement services to NHS 24.

TRAINING (continued)

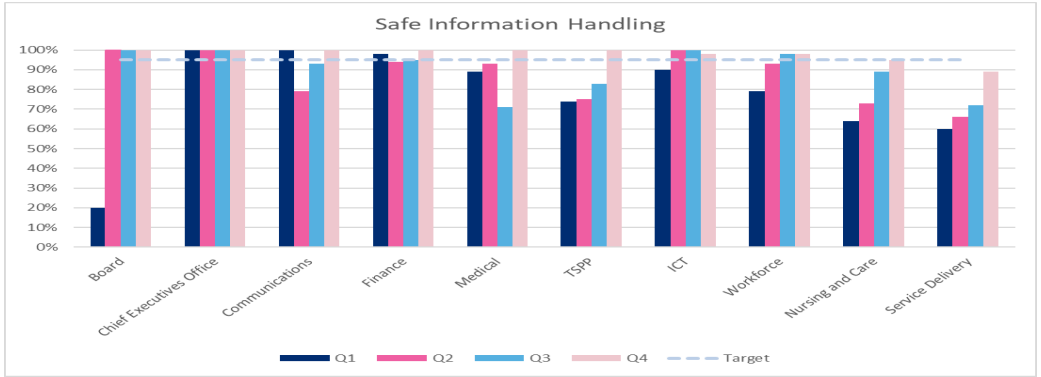
The compliance status for the Safe Information Handling (Data Protection) and the Stay Safe Online (Information Security) eLearning packages are displayed below showing continuous improvement over the year, though the 95% overall target, while close, has not yet been achieved, with SIH at 90.3% and SSO at 91.6%.

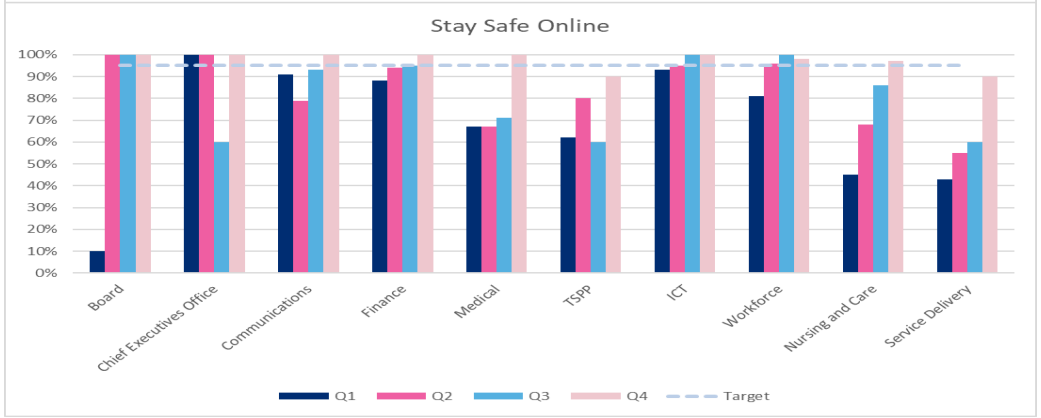




TRAINING (continued)

All Directorates have made progress towards the target, with the majority reaching or exceeding 95% by Q4. Service Delivery (as the largest directorate) has made very good progress throughout the year.





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 this period, 14 incidents were investigated by the Information Governance & Security Team, 3 were reported to the Health Competent Authority as a breach of NIS Regulations, and 1 was reported to the Information Commissioners Office.

NIS-R:

- BTs Managed MPLS network availability issue
- SAP Contact Centre availability issue
- Adastra / OneAdvanced Cyber Incident

ICO:

- Telephone number of Caller A was attributed to a subsequent Caller B, who in turn was referred to Police Scotland. As a result of this integrity issue, Caller A suffered significant distress.

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.

The following risks were closed over the period of this report.

Risk	Summary	Period	Status	Comments
RPND 025797	Information Asset owner training and responsibilities.	Q2	Closed	Closed in Q2 after training was delivered by an external facilitator.
RPND 029436	UK GDPR training non compliance, training to be completed with internal stakeholders.	Q2	Closed	Closed in Q2 after training was delivered by an external facilitator.
RPND 025796	Reputational damage due to email spoofing.	Q3	Closed	Controls available to NHS 24 have been implemented, including NHSInform, Care Information Scotland etc..
RPND 037567	Malware introduced via WiFi	Q3	Closed	Closed following the installation of the centralised WiFi solution, separating NHS 24 devices from guest devices.
RPND 037596	Malware introduced to NHS 24 estates via web browsing.	Q3	Closed	Closed following the introduction of 14-day patching and implementation of first batch of Attack Surface Reduction rules.

RISK MANAGEMENT (continued)

Risk	Summary	Period	Status	Comments
RPND 021405	Fail to evidence implementation of Records Management Plan.	Q3	Closed	Submitted evidence to National Records of Scotland in the Progress update Report (PUR).
RPND 037593	Undetected advanced persistent threat malware.	Q1	Closed	Closed following the introduction of 14-day patching and enablement of anti-malware detection.
RPND 042273	Service is impacted by a Denial of Service(DoS) attack.	Q3	Closed	Closed on implementation of DoS mitigation.
RPND 041263	Corporate devices compromised by home network and devices.	Q2	Closed	Closed following the introduction of 14-day patching and implementation of client firewall in the windows 10 roll out.

FINANCIAL IMPLICATIONS

There are no direct financial implications from this report, though it is expected that there will be financial implications from the 2023/24 work plans and for improvement works in relation to Data Protection and NIS-R legislation and physical security improvements.