**Digital &** **Information Governance**

Digital & Information Governance ensures necessary safeguards for, and appropriate processing of, patient and personal information. The nature of healthcare is that NHS staff encounter on a day to day basis, information which is both confidential and sensitive in nature. The usage of this information and the security of the systems the information reside in, is essential for the effective functioning of the health service as a public body, however within the governmental environment of the NHS there are number of key pieces of legislation which affect the everyday workings of the health board and the usage of this sensitive information. Some of these key pieces of legislation include:

* Data Protection Act 2018
* UKGDPR
* NIS Directive
* Public Sector Cyber Resilience Framework
* Freedom of Information (Scotland) Act 2002
* Public Records Scotland Act 2011
* Caldicott Report (1997)
* Common law of Confidentiality

Digital & Information Governance aims to help support the NHS Scotland Quality strategy to become safe, effective and person centred organisation and to do this we must ensure that we are maintaining confidentiality and upholding the data protection principles whilst also allowing access to information where appropriate to deliver the best possible care in an effective manner. Within the Board, there are specific measures and actions undertaken by the board in order to manage the risk and ensure that we can function effectively

**Reporting**

Within the board there is expertise for all of the aforementioned legislation within the Digital & eHealth department in order to provide advice and assistance, identify risks and actions to mitigate risks and recognise opportunities for development and increased security and safety for our information.

The Medical Director acts as Caldicott Guardian for the Board and has regular monthly meetings with the Head of Digital Governance/DPO. These meetings allow for discussions and updates around all aspects of digital and information governance and is also a platform for highlighting areas of concern that need to be addressed.

The role of SIRO (Senior Information Risk Owner) within the Board has been undertaken by the Director of Finance. The Head of Digital Governance has a dotted line reporting to the SIRO. The role of SIRO was created to provide board-level accountability and greater assurance that digital and information risks are addressed. The SIRO ensures that digital and information risks are treated as a priority for business outcomes.

The introduction of the EU General Data Protection Regulation (GDPR), in May 2018 and the subsequent UKGDPR, introduced on 1st January 2021, following the UK exit of the EU, strengthens the obligations on organisations. One of which is to appoint a Data Protection Officer (DPO). This role has been undertaken by the Head of Digital Governance within NHS Golden Jubilee.

The issues and decision making around Digital & Information Governance are reported through the Digital Governance Group which reports directly to the Clinical Governance Committee of the Board. An annual Digital & Information Governance Report will be produced and submitted to the Clinical Governance Committee.

The Digital Governance Group meets every quarter and is attended by representation from across the organisation including Executive Directors, Heads of Service and Service Managers. This group is chaired by the SIRO and co-chaired by the Caldicott Guardian. The group has remit to ensure that the Board has a robust Digital & Information Governance framework in place and offer opportunity to discuss digital and information governance issues. This group also offers peer support across the organisation, answering any information digital and governance questions and sharing good practice. An update report from the Digital Governance Group is submitted to the Audit and Risk committee on an annual basis. This report which includes details of any digital and information governance incidents which may have occurred and the actions taken to remediate, also contains details of FOI compliance which is in addition reported quarterly to the Senior Management Team via the corporate FOI lead. The update also contains details of any new developments, legislative change and service initiatives within digital and information governance to inform members and for further dissemination and discussion throughout the Board.

During 2022/23, a total of **35** information incidents have been recorded on Datix risk management system. **19** of these incidents were categorised as minor and **4** as negligible. Of the remaining **12** incidents, **11** are categorised as moderate and **1** categorised as major andare listed below.

|  |  |  |
| --- | --- | --- |
| **ID** | **Incident description** | **Severity Level** |
| 8540 | Further investigation of a quarantined email highlighted that clinical staff were sending documents to transplant coordinators via personal mailboxes and also WhatsApp. Although these documents do not contain patient identifiable information, they do contain enough information in relation to donor transplant that could potentially identify an individual. They do include staff details, hospital details, details of transplant process. IG attended department meeting to discuss the risks and highlighted the Board tools that are in place that will support this communication in a more secure manner. | Moderate |
| 8527 | Surgeon accessing clinical systems under other staff members logins. Caldicott Guardian sent a formal letter to the surgeon expressing this was against Board Policy and did not uphold appropriate and safe information handling. | Moderate |
| 8756 | Manager sent an OH staff referral to an incorrect Board distribution group, disclosing patient confidential information. Emailed was recalled and/or deleted following a notification email and staff member was made aware of the incident. | Moderate |
| 8911 | Patient entered level 5 booking office to hand in mail. This isn’t an isolated incident. Both security doors, East and West on Level 5 are unsecured resulting in anyone being able to enter level 5 and access all areas. Contractor immediately repaired doors and communication to advise that no locations or names should be given out to patients where the department is in a staff only area and should be directed instead to reception for them to contact the department. | Moderate |
| 9209 | Employee sent a personal WhatsApp message to colleague in relation to spouse being taken in to A&E at another Hospital and as a result would not be in work that day. The colleague (recipient of the WhatsApp message) spoke to one of the GJ cardiologists and asked them to have a look at the scans at the receiving hospital. The employee was made aware of this inappropriate request made by colleague. Staff reminded that this is breach of Board policy and data protection legislation. Letter sent advising of the severity of their actions and what the process will be if a breach happens again. | Moderate |
| 9233 | A clinical letter in relation to a consultant’s patient was incorrectly copied to another patient and verified by the consultant. Consultant was informed of this by the patient who incorrectly received the letter. Consultant informed patient. Increase vigilance when verifying clinical letters. Communicate issue within team as part of awareness raising. | Moderate |
| 9277 | Head of Department, with senior access permissions, logging onto PC and allowing members of department to use the PC under this login to log onto their emails. Password changed and staff now have access to separate PC. | Moderate |
| 9341 | Spoof email sent to HR acting as an Executive Director requesting update to bank details for payroll purposes. This was prevented by a member of the HR team after confirming this request with the Executive Director. Counter Fraud Services were notified and a Board wide Communication was circulated, making staff aware and to be cautious of spoofing emails. | Moderate |
| 9522 | MS Teams Channel, containing patient sensitive information on the sharepoint site of the channel, had been made public resulting in all users across NHS Scotland being able to access this site and the information. We were made aware of this by another Board. Channel was immediately made private and communication circulated. Alerts are set up by the national team to make each Board’s IG lead if a Team has been made public. | Moderate |
| 9710 | Discharge letters, generated by TrakCare, have been sent to an incorrect GP practice at another Board, this has happened across 10 NHS Scotland Boards to this same GP and practice. It would seem that if a GP is not selected against the patient on TrakCare, when the discharge letter is being generated it will default to the first GP on the list, this GP. Review of patients and updates made to correct practice, notified Business Services Manager to ensure staff are aware of this and select appropriate GP. | Moderate |
| 9802 | Theatre nurse returned to theatre during a procedure on a Face-Time call. Turned the phone to show the theatre and all present. Surgeon called out "That is a breach of patient confidentiality". Anaesthetist raised his head, statement heard by all in theatre Face-Time screen visible to Scrub and Surgeon. Ongoing Investigation to determine breach in policy/conduct. | Moderate |
| 9839 | Suspicious activity was detected by IT staff on an end user device and central file share. As a precaution the end user account, those associated with said user and access to the file share by all was disabled to allow investigation work to be carried out and prevent further contagion spread. The investigation found the presence of malware on both the user device and file share, likely cause was an infected USB Drive. This has now been contained with no further compromise to network or systems. Further review of content on devices to ensure no additional infection, exposed personal private healthcare work being carried out utilising Board resources and staff to support this. Ongoing HR investigation | Major |

There is a fully documented process and reporting structure to manage any Digital & Information Governance incidents within the Board which includes reporting to the Digital Governance Group chaired by the SIRO. Any significant incidents (Ranked Major or Extreme) must be reported to Scottish Government eHealth Directorate.

**Requests for Information**

In 2022/23, there were **84** FOI requests, an almost double increase from last year. **46** of these requests were responded to within the legislative timeframe. **38** were responded to out with the legislative timeframe, due to either the complexity of the requests or delays in receiving the information from the relevant department.

This is broken down as follows:

* Q1 – 11 requests. 9 responded on time, 2 late responses
* Q2 – 21 requests. 15 responded on time, 6 late responses
* Q3 – 22 requests. 16 responded on time, 6 late responses
* Q4 – 30 requests. 6 responded on time. 24 late responses

The following Subject Access Requests under the Data Protection Act 2018, were received:

* Q1 – 186 requests
* Q2 – 178 requests
* Q3 – 110 requests
* Q4 – 218 requests

Total = 692 requests

**National and Local Developments**

Through the involvement in these groups and the inclusion of digital and information governance within the Board’s Digital Strategy and delivery plan, there are a number of activities which were undertaken in 2022/23.These are described below.

1. **Cyber Resilience:   
     
   NIS Directive and Audit**  
     
   NHSGJ underwent a review of its compliance of the NIS Directive in October 2022, as part of the Scottish Health Competent Authority three year audit cycle, Year 1 audit (2020), Year 2 review (2021). The report, detailing the findings of October 2022 review have been shared with the Digital & Information Governance Group, Audit and Risk Committee and also to the Board Committee. A summary of this report is as follows;

|  |  |  |
| --- | --- | --- |
| **Overall Compliance**  **Status** | **2022** | **Amber 52%** |
| **2021** | **Amber 44%** |
| **2020** | **Amber 43%** |

Overall this was an improved submission with good progress in the controls implementation with 60% achieved or partially achieved.

Compliance status has been raised from 44% to 52%, with the risk exposure at 25%.

It was noted that the commitment of the board to cyber security is evident in the appointment of a Cyber-Security Operations Manager and the creation of additional posts, including the Cyber Security Compliance Officer, which is a post dedicated to manage the compliance of the NIS Directive and ensuring the controls within the NIS Directive Audit are owned and compliance met.

It was also noted that the staff awareness programme in cyber security is a strength of the board, an example of good practice with initiatives that may be of interest to other boards.

The second 3 year audit cycle has now commenced with the first year full audit over the following dates across 2023/24

* 24th May 2023 – Onsite Audit – To review site security and restricted access areas. Also an opportunity to demonstrate cyber and information security tools and applications.
* 15th January 2024 – Evidence submission deadline to auditor.
* 20th January 2024 – Staff meetings with key internal stakeholders. To discuss areas of compliance with appropriate subject matter experts and an opportunity to provide further evidence.
* 26th February 2024 – Receive interim report from auditor.
* 6th March 2024 – Management meeting to discuss content of interim report. An opportunity to ensure the report captures all findings.
* 11th March 2024 – Receive final report from auditor. This will include recommendations and areas of priority to be addressed.

Progress updates will be provided to the Board’s Digital & Information Governance Group and to the Audit and Risk Committee. Cyber Security is also now a Board standing agenda item.

Information/Cyber Security is highlighted as a risk on the Board’s risk register and taking into account the current intelligence on threat of cyber-attack and, in spite of the control measures and processes in place, it is recommended that the risk rating should remain as is currently recorded (12) within the Board risk register.

**SG Cyber Resilience Framework (CRF):**  
  
The [Scottish public sector action plan on cyber resilience](https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/) set out a commitment to develop a public sector cyber-resilience framework.

This framework aims to provide a consistent way for Scottish public sector organisations to:

* assess their cyber-resilience arrangements
* identify areas of strength and weakness
* gain reasonable confidence that they are adhering to minimum cyber-resilience requirements
* take informed decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis

In doing so, the framework seeks to:

* align with key wider cyber-related requirements under the UK General Data Protection Regulation (UK GDPR), the Security of Network and Information Systems (NIS) Directive and other standards
* minimise any additional burdens on Scottish public sector organisations, including by making clear how the framework relates to existing standards or requirements, and taking account of these when providing guidance on compliance
* provide a clear basis for internal and external audit and inspection activity, promoting greater consistency in the areas and issues covered by audit and inspection bodies when assessing Scottish public sector organisations
* help to provide clarity and assurance to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place across the Scottish public sector and its individual subsectors

These actions have been progressed and continue to be independently assessed as part of the NIS Directive Audit. The Board continues to meet the requirements of the Directive and the Framework through the Competent Authority audits.

1. **UK General Data Protection Regulation (UK GDPR)**The GDPR came into force on 25th May 2018 alongside the update of the Data Protection Act 2018 and the subsequent UKGDPR, introduced on 1st January 2021, following the UK exit of the EU and is the most significant changes to Data Protection legislation in over 20 years.

# The implementation of the UK GDPR has brought about key changes to data protection legislation which include:

# Increasing the rights for individuals

* + To be informed of data held by the Board
  + To have access to data held by the Board
  + To rectification where data held is inaccurate
  + To erasure of data (to be forgotten)
  + To restrict processing of data
  + To object to data being held
* Strengthening the obligations for organisations
  + To appoint a Data Protection Officer (DPO) for the Board
  + To ensure Privacy by Design – Data protection impact assessments must be completed prior to implementing new systems or processes
  + To mitigate risk when processing data by adopting measures
  + To implement an Information Asset Register detailing all information assets, including details of personal data held, where it came from and who it is shared with
  + To ensure contracts with Third parties who handle data on behalf of the Board, comply with GDPR regulations.
* Strengthening the management of breaches
  + To notify any breach of GDPR regulations to the Information Commissioners’ Office within 72 hours
  + To notify data subjects, whose data has been affected, without undue delay
  + To introduce and maintain a Personal Data Breach Register within the Board

# Significantly increasing the sanctions where organisations are not compliant

These sanctions can be up to €20 million or 4% or annual global turnover, whichever is higher.

During 2022/23, the Digital & Information Governance Team continues to work with the Board’s Information Asset Owners (IAOs) and supporting them with the review of their information assets and to support individual data cleanse work plans. IAOs are required to submit twice yearly progress reports on the Information Assets for which they have responsibility to the Board’s Information Governance Group.

Work also continues with IAOs and project managers working with the Digital & Information Governance Team to carry out Data Protection Impact Assessments (DPIAs), this upholds UK GDPR requirements in relation to Privacy by Design and allows the necessary risk assessment to be carried out at the very early stages of changes to data processing or introduction of new systems. This then identifies where there is a need to have in place a data processing or data sharing agreement, which is a requirement under the UKGDPR.

The Board’s Data Protection Officer continues to work with the IG Leads across NHS Scotland, including the Central Legal Office, to ensure that the documents used to support the data processing are legally adequate in line with the UK GDPR.

1. **Information Commissioner’s Office (ICO) Audit**

In November 2022 NHS Golden Jubilee was audited by the Information Commissioner’s Office (ICO). ICO are our regulators for compliance with Data Protection and the UK General Data Protection Regulation (UK GDPR).   
This audit was carried out across all 22 NHS Scotland Health Boards.

At the beginning of November 2022, the Board submitted evidence of compliance across the following areas within the scope of the audit:

* Management structures
* Policies and Procedures
* Training/Informed decision making for data sharing
* Processor contracts
* Record(s) of processing activities
* Transparency
* Data protection impact assessments/Assessing the legality, risks, and benefits of sharing data
* Personal data breaches
* Information Sharing Agreements and Logs

Interviews with key internal staff then took place over 3 days, 24th, 25th & 29th November 2022, with further information provided to the audit team by these staff.

An interim report was received on 15th December 2022 with an agreed final report and action plan received on 12th January 2023.

A summary of the report is as follows:

* An overall assurance rating of reasonable
* 76% assurance across high and reasonable (59% & 17% respectively)
* 17% limited assurance
* 7% very limited assurance

A total of 12 recommendations received (2 urgent, 5 high, 4 medium 1 low)

Of those recommendations:

67% are completed

80% of the urgent recommendations are completed  
64% of the high recommendations are completed  
55% of the medium recommendations are completed  
100% of the low recommendations are completed  
  
We are currently on target for completion of all recommendations by December 2023.  
Progress updates have been provided and will continue to be provided to the Executive Leadership Team, Audit and Risk Committee and to the Digital and Information Governance Group.

There is no scheduled follow up from ICO, however, they may contact Boards for a progress update.  
ICO will publish an overall NHS Scotland exceptions report on their website once all Boards audits are completed. This report will not include any specific Boards results.

1. **Public Records Scotland Act 2011**

The Public Records (Scotland) Act 2011 came into effect in January 2013. In order to comply, we were required to prepare and submit a Records Management Plan (RMP) setting out proper arrangements for the management of the authority’s public records to the Keeper of the Records of Scotland. The Board’s Plan was submitted and approved on April 2017. The Board continues to monitor compliance with the RMP through updates to the Digital & Information Governance Group and to the National Records Management Forum.

The Board has also submitted 4 Progress Update Reviews to The Keeper’s Assessment Team and has recently been invited by the National Records of Scotland (NRS) to submit a Progress Update Review (PUR) for this year, to be submitted by **31st July 2023.**

The Progress Update Review (PUR) mechanism was announced in the Keeper’s 2016 Annual Report and has been developed in partnership with a Stakeholder Forum. Formally launched on 14 December 2016 the PUR mechanism is intended to help authorities demonstrate their continuing compliance with s.5(1)(a) of the Public Records (Scotland) Act 2011 (the Act) to keep their RMPs under review. It is also an opportunity for the Board to highlight and share with The Keeper’s Assessment Team the advances being made in the provision of our records management services and to receive impartial feedback and advice on those advances by the Assessment Team.

The PUR is a wholly voluntary scheme; there is no obligation under the Act for authorities to submit a PUR, however, the Board submitted their last PUR in 2022, with very positive feedback from the team at NRS. The Board has accepted this invitation and will submit a Progress Update Review by the deadline outlined above.

The outcome report from NRS will be shared with the Digital & Information Governance Group.

The Board’s Records Management Plan and PURs are available to view on the Board’s external website.

1. **Scottish Government Records Management Code of Practice (CoP)**The current 2020 version of the Records Management CoP is being reviewed and updated. This review also includes a scoping exercise for a digital, dynamic platform to host the CoP, making it easier for users to navigate through the information.

This work is being led nationally by a representative within Scottish Government with input from all Records Management and Information Governance Leads across NHS Scotland.

Delivery Groups and Digital Platform Groups have been stood up with significant work underway to redesign and update the CoP.

Although part of the review is to scope an appropriate digital platform for the CoP, this will take a few years before being fully implemented.

1. **Microsoft 365**NHS Scotland are contracted under a single Microsoft 365 tenancy. This means that the whole of NHS Scotland is attached to one domain making it easier to share necessary information, in a safe and secure manner across this tenancy. This also means that there is a need to ensure border control across Boards and that there are controls in place to manage data processing and access rights.

This processing is managed nationally as a “once for Scotland” approach with representatives from all digital and information governance disciplines involved in the risk assessing and approval process.

Documents, such as Data Protection Impact Assessments, Information Sharing Agreements, System Security Policies to name a few, are reviewed and approved nationally and adopted at Board level to support the use of Microsoft 365 and the various approved apps available, such as Teams.

These documents are circulated to the Information Governance Group, SIRO and Caldicott Guardian for local review and approval.

**Training and Education**

1. Staff Induction

Upon commencing employment within the Board, all staff must attend an online one-day corporate induction event. This induction also includes a dedicated section to digital and information governance, which was developed by the Head of Digital Governance. This training ensures that staff understand the importance of digital and information governance and their responsibilities as an employee. The session is interactive and allows staff members to use scenario based learning to consider and relate digital and information governance issues to their own areas of work.

2. Mandatory Training

The **Safe Information Handling Module** is a mandatory bi annual e-learning course, which must be undertaken by every member of staff. It is designed to give information about the basic principles of data protection; guidance on good practice and sources of advice and further information. Reporting on compliance rates for mandatory training are included in the Board’s Integrated Performance Report. The target for compliance is 90%, the overall compliance rate for 2022/23 was **81.4%.**

3. Cyber Security Training  
Cyber-security awareness campaigns were run over the month of October 2022. This included regular awareness notices circulated to staff by Corporate Communications, cyber-awareness posters in staff areas with key messages including password safety and phishing awareness. A new Foundation Level Cyber Security Training Module is currently being developed. This module will be aimed at all staff to complete and currently working through the documentation for approval to a mandatory module. The aim is for the module to be completed by the end of quarter 2 and after a successful pilot, in place for the end of the calendar year.

4. Information Asset Training

This continues to be delivered to the Board’s Information Asset Owners (IAOs). This specific training focuses on information asset management and best practice guidance. All IAOs, who have been trained, have signed a Declaration outlining their responsibilities as IAOs.  
The training has now been developed and delivered to Information Asset Administrators (IAAs). The training continues to be delivered to IAO/As via Teams approx. every 8 weeks.

**Communication**

The Board continues to receive a number of ‘malicious’ emails which constitute attempted malware attacks, where a link or attachment containing a virus is added to the email encouraging the recipient to click on the link or open the attachment.

As well as additional technological control measures, we continue to raise awareness of the potential threat of attempted malware attacks through communications issued to staff on a frequent basis in the form of weekly updates as well as daily “All Staff” emails to remind staff of the importance of not responding to these emails with clear instruction on how to deal with them. In addition, updates in the Staff Bulletin have been distributed and posters have been designed and distributed as a visual reminder to staff regarding this ongoing potential threat.

The internal controls that ensures digital and information governance is adhered to throughout the organisation is through the creation and maintenance of policies to ensure that staff have relevant, up to date and accurate advice and assistance to help them carry out their role. These policies are maintained on a central document location called Sharepoint where they can be accessed by any member of staff. These are updated, in line with the latest government guidance and best practice advice, every two years.

Board Members and Senior Management are kept updated with digital and information governance and cyber-security developments and changes through the presentation of papers at the Board, Audit and Risk Committee, Digital & Information Governance Group and on an ad hoc basis. Staff are also alerted to changes which affect them through e-digest updates and email communication.

This multi-pronged communication approach helps to ensure there is awareness within the organisation around digital and information governance and cyber-security and the key points of contact identifiable.

Digital & Information Governance is a support measure to ensure that the Board can carry out its public function whilst also complying with its legal responsibilities in terms of information management. It provides safeguards and recommendations through policies and practices and provides reassurance to staff and patients that their sensitive information is utilised in the most appropriate way. All of the aforementioned steps from new developments to training and communication all help to assure that strong digital and information governance is in place within the Board.

**Work plan**

Information Governance is included in the Board’s eHealth delivery plan and progress is reported to the Senior Management Team.