Approved by Committee on 11 November 2024

Information Governance Committee
Monday 2 September 2024 at 9.30am
MS Teams meeting

Present:	Mr Marc Mazzucco, Non-Executive Board Member (Chair) Ms Sheila Cowan, Non-Executive Board Member (Vice Chair) Mr Neil McAleese, Non-Executive Board Member – part meeting Cllr Douglas Reid, Non-Executive Board Member
Ex-officio:	Ms Claire Burden, Chief Executive and Senior Information Risk Owner Ms Nicola Graham, Director Infrastructure and Support Services Dr Crawford McGuffie, Medical Director, Deputy Chief Executive and Caldicott Guardian
In attendance:	Mr Martin Duggan, Cyber Security Manager item 6.1 Mr Derek Gemmell, Acting Assistant Director, Digital Services items 6.1 and 7.1 Ms Natali Higgins, Information Governance Manager (Corporate Records) item 6.2 Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Apologies for absence

1.1 Apologies were noted from Mrs Jean Ford, Ms Linda Semple and Ms Ann Catherine Wilson.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 29 April 2024

3.1 The minute of the meeting held on 29 April 2024 was approved as an accurate record of the discussion.

4. Matters Arising

4.1 The action log had previously been circulated to Committee members and all progress against actions was noted. The following areas were highlighted:

Item 6.1 (29/04/24), Cyber Security update – Ms Graham advised that she had responsibility for the action related to identification of funding for a National Cyber Security Centre accredited cyber incident response provider. She added that this was being looked at as an area of risk to be added to the Digital budget. **NG**

In reply to questions from members, the Medical Director, Dr Crawford McGuffie, gave assurance that while the Information

Governance (IG) team continued to experience workforce challenges, the position was improving and areas of risk related to the IG work programme were being actively managed. The Medical Director would discuss progress of individual actions with the Committee Chair outwith the meeting and short narrative would be added to update on progress with actions. **CMcG**

4.2 **Information Governance Committee (IGC) Work Plan 2024** – Committee members noted the draft work plan.

5. Risk

5.1 Information Governance Strategic Risk Register

The Medical Director, Dr Crawford McGuffie, presented the Risk Register report covering the period up to July 2024. The report was discussed in detail at the Risk and Resilience Scrutiny and Assurance Group meeting on 19 July 2024.

Dr McGuffie provided details of the three risks allocated to the IGC shown at Appendix 1 of the report. Appendix 2 gave further details for each risk. Appendix 3 provided details of the risk severity consequence matrix. There were no proposed risks for escalation or downgrading for this meeting and no emerging risks.

Committee members received a detailed update on the work being done to mitigate the very high risk being tolerated related to COVID-19 Inquiry, retention of mailboxes for key decision-makers. Mitigations included the use of leavers' flow charts, ongoing audit of e-mail accounts and identification and quantification of historical mail boxes for staff who left the organisation between February 2020 and January 2024.

In response to a question from a member, Dr McGuffie advised that a review of Risk ID 557, Compliance, Information Governance, was in process and an update would be provided at the next meeting. The Director of Infrastructure and Support Services clarified in reply to a question from a member that the level of risk related to Risk ID603, Service/Business interruption, Cyber incident, was determined based on the risk reporting template used. She reassured members that this high risk was being managed appropriately.

Outcome: Committee members noted the report and took assurance from work being done to manage strategic risks which fall under the committee's governance remit.

5.2 There were no risk issues to report to the Risk and Resilience Scrutiny and Assurance Group.

6. Information Governance

6.1.1 Cyber Security update

The Acting Assistant Director, Digital Services, Mr Derek Gemmell, provided an update on key areas of activity undertaken by the Cyber Security team over the last Quarter.

Mr Gemmell advised that the organisation continued to remediate vulnerabilities and ensure devices were patched and as up-to-date as possible. There was nothing significant to report in terms of alerts. The Board had introduced a new security product to virtually patch servers where operating systems were no longer supported, as the software packages currently used by the Board were not compatible with updated MS operating systems. All products were being reviewed to look at integration of older applications (apps) with existing major apps.

NHSAA was one of six pilot Boards in Scotland for MS Security Baseline, with the aim to apply secure controls against Windows 10 and 11 across the NHS Scotland Tenancy. Following a successful pilot, this would be rolled out across the Board, with work expected to be completed by end-September 2024.

Members were advised that cyber security awareness training had moved to a new module on Turas. There had been some national issues with linking accounts between Learnpro and Turas so it was not possible to provide up-to-date training uptake information at this time, however, this should be available for the next meeting.

Mr Gemmell advised that an organisation Crisis simulation event had taken place on 29 August 2024, with over 200 members of staff in attendance. This successful event had raised awareness of how the Board needs to react under any crisis situation. Mr Gemmell updated that for the internal audit on cyber security and resilience, the three outstanding advisory actions had been passed to the auditor for closure and a response was awaited. An update on the Network and Information Systems audit 2023/24 audit and Digital strategy audit would be provided later in the meeting.

Mr Gemmell advised in response to a question from a member that focused work was taking place to encourage staff who had not already done so to bring in their laptops to allow changeover to Bitlocker encryption. Direct communication was being issued to staff to let them know that should they fail to comply with this requirement their laptop would cease to function. The Director of Infrastructure and Support Services, Ms Nicola Graham, added that all of the Board's laptops currently had encryption and the Board was moving from McAfee to Bitlocker as part of the MS suite of products being used going forward.

Outcome: Committee members noted the summary of the Cyber Security team's activities.

6.1.2 **Cyber Security team progress in planning for 2024 Network and Information Systems (NIS) audit**

Mr Martin Duggan, Cyber Security Manager, provided an update on the 2023 NIS audit summary and the Cyber Security team's progress in planning for the 2024 NIS audit.

Mr Duggan advised that this was the first year of a three year plan. The Board had achieved an overall compliance status of 87%. Of the 427 controls, all 17 categories and 61 of the 68 subcategories achieved a compliance of 60% or more. 14 of the categories, and 53 subcategories were rated at 80% compliance or above, with 10 at over 90%. 351 of the 427 controls achieved (82%). In 2023, 30 subcategories had been marked as complete, with a total of 145 controls. The Board achieved two of the more advanced 80-80-0 key performance indicators, with a third close to achievement, only being prevented by the single subcategory with less than 30% compliance.

Mr Duggan advised that intermediate audits would take place in 2024 and 2025 covering the 72 controls against which the Board had not achieved full compliance. The main area of focus would be on business continuity and disaster recovery. An action plan had been developed, shown at Appendix 1 of the report, including timescales for completion. Progress to date included the recent crisis simulation event, as noted above, and testing of Trakcare hosting environment in April 2024, both of which would be provided as evidence for the audit.

Members received a detailed update on the 2024 control management approach to be adopted, as well as areas of challenge. As detailed in the report, there were four controls which would be challenging to achieve related to sanitisation of data from devices before disposal and use of generic accounts, and a change of policy and working may be required to address these areas. The report gave details of predicted compliance with controls by February 2025.

Committee members discussed Appendix 1 of the report and requested that further narrative be provided in relation to the business continuity/disaster recovery testing plan 2024 to enable Committee to monitor status and progress in the completion of actions. **NG/MD**

Outcome: Committee members welcomed the overall progress made in 2023 and noted the update on planning for the 2024 NIS audit.

6.2 **Information Governance (IG) Update report**

Ms Natali Higgins, Information Governance Manager (Corporate Records) provided an assurance report in respect of the Board's IG obligations and the following areas were highlighted:

6.2.1 **Public Records (Scotland) Act (PRSA) 2011 – Corporate Records Management update**

Element 4, Business Classification Scheme, and element 11, Audit Trail, remained at amber status. The national team was in the process

of recruiting to a Records Manager post to take this work forward. Once the post was in place, they would notify Boards of the Once for Scotland approach and the organisation would be able to progress elements 4 and 11.

For element 15, Public records created or held by third parties, this remained at amber status. Work required for this element had been combined with work needed for A06 of the Information Commissioner's Office (ICO) action plan, as under both DPA and PRSA the Board required to ensure appropriate terms and conditions in all contracts where processing of information was carried out. This work had unfortunately been delayed. All other elements of the plan had green status.

Ms Higgins provided an assurance update on progress with implementation of the Board's Records Management Plan (RMP). She advised that considerable work was ongoing within Directorates to improve records management. Four areas had green status and four areas had amber. Six areas had red status. Areas of main concern related to East Ayrshire Health and Social Care Partnership (EA HSCP), which had not submitted a plan, and Finance and Pharmacy which had made little progress. Pharmacy had recently identified a new Champion and once established, this should enable work to be progressed more quickly. Significant work was ongoing within Acute services which was commendable given the service pressures faced.

Ms Higgins emphasised the importance of all Directorates having RMPs in place to ensure efficiency, good operations, to comply with legislation and to enable M365 implementation. Ms Higgins had recently met with Champions to update them on national recruitment and plans to move to Sharepoint. She had encouraged Directorates to be as prepared as possible to avoid harsh deadlines.

Following submission of the Board's progress update review (PUR) report in March 2024, Public Records Scotland (PRS) had provided a draft report, noting the hard work being done by the Board to bring elements of records management arrangements to compliance. PRS would like to see further update on elements 4 and 11. However, that work was being led nationally and the Board would like to follow the Once for Scotland approach in order to make the Sharepoint rollout most effective.

6.2.2 **Information Security Incident Report**

There were 25 incidents during the reporting period which was in line with the quarterly average based on data over the last three years. There were no personal data breaches and no complaints under investigation by ICO during this reporting period. Following usual trends, most breaches occurred in Acute services due to the size of the department, staff numbers and sensitivity of information held. In discussion with colleagues there were no significant incidents to report.

6.2.3 **Freedom of Information (FOI) update and six monthly report**

There had been a slight decrease in the number of FOI requests compared to the same period in 2023 although the volume of requests remained high. Compliance had reduced from 92.9% to 90.8% which was rated as good by the ICO. A new Information Assurance Officer had been recruited to the team to support the FOI work plan and ensure compliance rates are improved and maintained.

The Medical Director, Dr Crawford McGuffie, advised in response to a question from a member about the number of FOI requests from MSP researchers, that there was a need to balance the right to access information with the pressures being placed on Boards. This was a standing item at quarterly meetings between the Chief Executive, Medical Director and MSPs. Cllr Reid would also raise the issue through EA Council meetings with MSPs.

6.2.4 **Record of Processing Activity update**

The position was as reported at the last meeting, with work ongoing to move all information assets from the current register and prepare them for import to One Trust.

6.2.5 **IG work programme 2024/25 update**

Ms Higgins highlighted progress updates related to FOI, with two new actions added related to training for new IG team members, which should both be completed by the next reporting cycle. The team continued to support implementation of M365. Although resource was now in place nationally to support this action, no new national compliance documents had been produced. An update on ICO Audit action A06 was provided below.

6.2.6 **Information Commissioner's Office (ICO) action plan –**

Committee members received an update on progress with the ICO action plan.

For Action A04, related to review of policies and procedures, work was required to ensure all the organisation's controlled documents are up-to-date. This required an update to the controlled document policy which was currently ongoing with the document's owner. The IG team had developed a communication plan and once the policy had been reviewed and approved it would be circulated widely across the organisation.

For Action A06, to ensure all processors comply with terms of written contracts, the actions related to development of a DPA log and adoption of the use of OneTrust were complete. Some progress had been made with the action for the IG team to meet regularly with the Procurement team although further discussion was required between the Head of IG and Head of Procurement. Ms Higgins highlighted

that, as previously reported, this action would involve a significant amount of work and resources from IG, Procurement and other services to be involved. Once the IG team was back to full complement a plan would be put in place to support this significant piece of work.

The Medical Director, Dr Crawford McGuffie, thanked Ms Higgins and the wider IG team for their support to ensure the Committee meeting could take place, particularly given the current pressures facing the team. The Committee Chair, Mr Marc Mazzucco, reiterated his thanks to the team for the good work being done in difficult circumstances.

Outcome: Committee members noted the report and took assurance from the work being done to promote compliance with the relevant legislative frameworks.

7. Audit

7.1 Digital Strategy internal audit

The Acting Assistant Director, Digital Services, Mr Derek Gemmell, presented the Digital strategy internal audit to members for information. The auditors had given a minor improvements required rating and identified four improvement actions, with three related to compliance with existing procedures. Evidence related to two actions had been submitted, with further evidence submitted in August 2024 to allow closure of another action. One action would remain open until October 2026 when the new Digital strategy would be drafted. Progress with the improvement action plan was being monitored through the Integrated Governance Committee, as lead Governance Committee for this audit report.

Outcome: Members noted the Digital Strategy internal audit and were encouraged by the actions taken.

8. Corporate Governance

8.1 Information Governance Operational Delivery Group

As the last scheduled meeting was cancelled there were no minutes to report. Dr McGuffie advised that group meetings had been impacted due to IG team workforce pressures and he would discuss this and other priority areas with the IGC Chair, Mr Marc Mazzucco, outwith the meeting. **CMcG**

9. Key issues to report to NHS Board

9.1 Committee members agreed that the following key issues be reported to the NHS Board meeting on 7 October 2024:

- Risk register – No change to risk ratings and some updates

due.

- Cyber Security – focused work to upgrade staff laptop encryption to Bitlocker.
- NIS audit progress update.
- NHSDG cyberattack – importance of having robust cyber security measures and corporate records management process.

10. Any Other Competent Business

10.1 **NHS Dumfries & Galloway (NHSDG) Cyber Attack** – In response to a question from a member, the Medical Director, Dr Crawford McGuffie, advised that the Corporate Management Team had recently received an update from the Medical Director at NHSDG on the cyberattack at NHSDG and its impact. The Director of Infrastructure and Support Services, Mrs Nicola Graham, reassured members that NHSAA had multi-factorial authentication on a single VPN. She underlined that it was important for Boards to understand why the cyberattack was able to take place to identify any learning.

The Committee discussed the significant impact of the cyberattack at NHSDG. Members discussed the importance of having effective digital cyber security measures in place, alongside a robust corporate records management process to minimise risk and ensure that the Board held appropriate information in a secure manner.

11. Date and Time of Next Meeting
Monday 11 November 2024 at 9.30am, MS Teams meeting

Approved by the Chair, Mr Marc Mazzucco Date: 11 November 2024