Approved by Committee on 12 May 2025

Information Governance Committee
Monday 24 February 2025 at 9.30am
MS Teams meeting

Present:	Mr Marc Mazzucco, Non-Executive Board Member (Chair) Ms Sheila Cowan, Non-Executive Board Member (Vice Chair) Mrs Jean Ford, Non-Executive Board Member Mrs Sharon Morrow, Non-Executive Board Member Cllr Douglas Reid, Non-Executive Board Member
Ex-officio:	Ms Claire Burden, Chief Executive and Senior Information Risk Owner Mrs 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 Ms Marie Lynch, Interim Head of Information Governance and Data Protection Officer Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Welcome / Apologies for absence

1.1 The Committee Chair, Mr Marc Mazzucco, welcomed Mrs Sharon Morrow, new Non-Executive Board Member, who was attending her first Information Governance Committee meeting since joining the Board in January 2025.

1.2 Apologies were noted from Mrs Lesley Bowie.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 11 November 2024

The minute of the meeting held on 11 November 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. Committee members received an update on the following actions:

Item 6.2.4 (11/11/24), Freedom of Information (FOI) update - Dr McGuffie advised that he had recently written to MPs and MSPs about the volume of FOI requests being received. He would raise this

at the next quarterly meeting and provide an update at the next Committee meeting. Action ongoing.

Item 6.1 (11/11/24), Cyber security update – the report and dashboard had been updated in response to comments from members. Action complete.

All other items were either on the agenda, a date was scheduled for the discussion or the action was complete.

4.2 **IGC Work Plan 2025/26** – Committee members noted the work plan.

5. Risk

5.1 Information Governance (IG) Strategic Risk Register

The Medical Director, Dr Crawford McGuffie, presented the Risk Register report. A version of the report was discussed in detail at the Risk and Resilience Scrutiny and Assurance Group meeting on 24 January 2025.

Members received an update on the two IG risks. There was one very high risk ID 557 being treated related to compliance with IG. The risk had been extensively reviewed since the last meeting, with no change to the risk grading and ongoing plans for the team to further refine the risk. The risk was due for review on 30 April 2025.

There was one high risk ID 603 being treated related to service/business interruption – cyber incident due to the ongoing threat of cyber incidents. An improvement action plan was in place for the Network and Information Systems (NIS) audit 2024 which aligned with the 2025 audit. The risk was due for review on 30 April 2025.

Members received assurance that both risks were being managed effectively. There were no emerging risks to report and no proposed risks for escalation or termination.

Dr McGuffie advised in response to a question from a member related to risk ID 557, that the Learnpro system sent reminders to individual staff on compliance with mandatory training. Compliance reports were also shared at Corporate Management Team (CMT) meetings, as Directors explicitly held responsibility and risk related to staff completion of mandatory training. The risk was now being reviewed more regularly, moving from six monthly to quarterly review.

In reply to questions from members about risk target timescales, Dr McGuffie advised that following the Board Risk workshop held in August 2024 and outputs agreed, improvement work was being taken forward and iterative progress continued to be made in relation to reporting of risk. Mrs Jean Ford, in her role as Audit and Risk Committee Chair, advised that improvement work was ongoing with a view to taking a consistent approach in regard to risk target

timescales across the organisation. She clarified that a short life working group had been set up to look at risk appetite. Wider risk improvement work was being done based on audit recommendations and discussion with the team.

The Director of Infrastructure and Support Services, Mrs Nicola Graham, advised in reply to questions from members regarding risk ID 603 that she did not expect the risk status to change. The position was challenging due to emerging cyber security risks and work continued to mitigate and maintain the risk at its current level. She explained that this was a high risk due to the potential impact of a cyber security attack.

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 Cyber Security update

Mr Martin Duggan, Cyber Security Manager, provided an update on key areas of activity undertaken by the Cyber Security team. The report's format had been revised following discussion at the last Committee meeting, with a new dashboard provided showing the Cyber Security team's activities, along with relevant key performance indicators (KPIs).

Mr Duggan highlighted key areas of monitoring activity:

- NHSAA was the first Board to successfully complete the implementation of all features within the NHS Scotland mandated Microsoft Security Baseline rollout.
- There had been an upgrade of Sonicwall VPN appliances to address new and actively exploited critical vulnerability.
- Cyber Scotland Week would run from 24 February to 2 March 2025. This would be advertised on the Board's Cyber Security Sharepoint site, Daily Digest, eNews and Viva Engage and a reminder to staff to complete cyber security and MAST training.
- As detailed in the report, 10,174 staff had completed cyber security training at 1 February 2025, with 83% compliance. Compliance rates by Directorate were detailed in the report.
- The Board had submitted evidence for the Network and Information Systems (NIS) audit on 3 February related to the controls not been met last year. The audit involved significant work for the department and wider organisation. The report outlined the work that had been done related to business continuity and disaster recovery (BC/DR) planning and the exercise completed in December 2024 which should address a

number of these controls. The auditors would meet with staff on 13 March 2025 to discuss key areas for the audit.

Mr Duggan advised in reply to a question from a member that it was not possible to include KPIs for some activity, for example, cyber security training, as this varied from month to month.

Mr Duggan clarified in reply to a query from a member on the BC/DR exercise schedule 2025-2027 that it was correct that the same ransomware tabletop exercise was planned annually as this was currently the highest cyber security risk to any organisation.

Committee members welcomed the update on cyber security activity outlined in the dashboard. Members requested that brief narrative be provided alongside the dashboard in future reports to give context to the work being done, including areas where the Board is performing well and work taking place to address any issues, to promote understanding and enable the Committee to effectively monitor progress. **NG/MD**

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

6.2 **Information Governance assurance report**

The interim Head of Information Governance and DPO, Ms Marie Lynch, provided the IG assurance report covering the following areas:

6.2.1 **Public Records (Scotland) Act (PRSA) update**

Members received an update on NHSAA's compliance with PRSA and progress with the corporate records management (CRM) plan. There were currently no red Elements and three amber Elements, with all other Elements green. Members received a detailed update on the three amber Elements:

Element 4, business classification scheme (BCS) - the Board had adopted a national NHS Scotland BCS developed by the NHS Scotland Records Management Forum. A BCS across all Boards was being considered as part of M365 and Sharepoint implementation. This work had begun and an outline plan was due by May 2025 with target completion date in March 2026.

Element 11, audit trail - this would remain amber until Sharepoint had been implemented nationally with robust audit trail functionality.

Element 15, public records created or held by third parties - contractual clauses regarding the management of information and records had been added to the Board's standard terms and conditions to support compliance. Further work was required at service level to ensure that these clauses were added to new and ongoing contracts where appropriate. It was intended to undertake this work in

conjunction with action A06 on the ICO action plan; that the organisation takes accountability for ensuring all processors comply with the terms of written contracts. As previously reported, this would involve a significant amount of work form Procurement and other services.

Ms Lynch provided an update on compliance with Directorate improvement plans. Overall compliance had increased, with 53% compliance in quarter 3. Directorates with low compliance were aware and would take action to improve the position. She outlined the significant work that continued to ensure appropriate organisational measures were in place to implement good records management practices, as detailed in the report.

The Board had not yet been invited to submit a Progress Update Review (PUR) for 2024. The report for 2023 noted that the Board continued to take its statutory obligations seriously.

Committee members discussed Directorate records management improvement plans, particularly those with low compliance, and supported the focused approach being taken to address these areas, with quarterly monitoring and reporting through CMT. The Medical Director, Dr Crawford McGuffie, advised in reply to a question from a member that for EA HSCP, the Director was looking at potential areas, such as reporting mechanisms, to improve compliance and progress would be reported via CMT.

In reply to a question from a member about progress with implementation of file plans, Ms Lynch advised that each Directorate had a records management champion in place who met regularly with the CRM Manager, with significant support provided in relation to CRM. Dr McGuffie explained that it could take longer for larger Directorates to complete this work due to the volume of work involved.

Dr McGuffie provided assurance in response to comments from members that the report had iteratively improved taking on board feedback from the Committee. Significant work was taking place across the organisation to ensure continuous improvement in relation to corporate records management and the report reflected an overall positive position.

The Committee requested that future reports provide short narrative on the continuous improvement approach being adopted to give context to the compliance data, including expected completion timeframe for work, key areas of risk and mitigations in place to enable the Committee to effectively monitor progress. **CMcG/ML**

6.2.2 **Information Security Incident Report**

Members received an update on information security breaches which had occurred within NHSAA in quarter 3, October to December 2024.

There were 19 breaches during the reporting period which was lower than the average of 25 breaches based on data over the last three years. There were no breaches considered notifiable to the Information Commissioner's Office (ICO). Since the paper was submitted, the ICO had informed the Board that they had closed a breach reported by NHSAA in 2023 related to highly sensitive information being shared with the wrong recipients. There had been a delay in responding due to a backlog at ICO. The Board awaited the outcome of breaches reported to ICO in 2024.

In quarter 3, the ICO received one complaint related to NHSAA processing of personal data. This breach did not meet the criteria for reporting to ICO and face-to-face training was provided to the department. The ICO was satisfied with the action taken and had closed the complaint. Further information security breach trend information was provided in Appendix 1 of the report.

Ms Lynch advised in response to a question form a member that there was no national data currently available to enable comparison of breaches in other Board areas and she would raise this at national level. **ML**

6.2.3 **Freedom of Information (FOI) Annual Report**

Members received the FOI annual report 2024 which provided full analysis and oversight of FOI requests, response times and use of exemptions. The Board used the same methodology as ICO to enable comparison.

In 2024 there were 975 FOI requests responded to, a slight decrease compared to the previous year. 30% of requests received had to be sent to more than one directorate for response. The Information Team fully or partially answered 15% of all requests responded to in 2024. For an additional 14 requests the information was not held by them. Within this time period, 882 requests were responded to within the statutory 20 working days, with 93 late responses. There were eight requests for internal review and the Board's decision had been upheld in all of these cases, with all responded to within the 20 working day statutory timeframe.

The continued volume of requests, as well as organisational pressures across the Board, had impacted on the compliance rate which had reduced from 92.9% in 2023 to 90.5% in 2024, rated as good performance by Office of the Scottish Information Commissioner (OSIC). The introduction of a new 0.5 whole time equivalent Information Assurance Officer had ensured that rates were maintained and did not reduce further. To date, FOI requests in 2025 were similar to 2023 which had been the busiest year.

The Board had received a decision from the OSIC on an appeal notified to the Board in 2022. The decision was partially in favour of the Board and they had agreed with the use of exemptions in some cases and in others the Board was required to release information.

Committee members discussed the report and commended the team for their performance and significant work being done to respond to FOI requests, particularly given the large volume of requests received.

Dr McGuffie advised in reply to a question from a member that he had written to MPs and MSPs about the high number of requests being received from four researchers and would discuss this at the next quarterly meeting with MSPs and report back to the Committee. Consideration will be given as to whether modelling the associated costs with the rise in FOIs is possible. The Committee would continue to monitor the position closely.

6.2.4 **IG work programme update**

Members received an update on the IG work programme and progress against key areas of work ongoing in the following areas:

- **PRSA** – implementation of records management plan – required actions related to adoption of BCS; destruction arrangements; audit trail; and public records held or created by third parties. Progress reported in detail above.
- **FOISA** – provision of training for new IG Assurance Officer and IG Analyst; and supporting implementation of M365. Induction to be completed by 31 March 2025.
- **ICO Audit action A04** – review of policies and procedures - awaiting publication of Controlled Document policy, target completion date August 2025.
- **ICO audit action A06** – to ensure all processors comply with terms of written contracts. As previously reported, this involved significant work. Some resource had been dedicated to transferring assets to One Trust. Should this progress continue, target completion date to be September 2025.

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

7. Corporate Governance

7.1 **Information Governance Committee Terms of Reference Annual Review**

Committee members reviewed the Terms of Reference with no changes made.

There was discussion on representation from the Head of Health Records at Committee meetings to give assurance of the management of health records. Members were content that the Committee's decision in November 2022 to report Health Records Services activities that fall within the remit of the Board's IG function

to the Information Governance Operational Delivery Group should stand, with exception reporting to the Committee as required.

Outcome: Committee members reviewed and supported the ToR with no changes made, for onward submission to the NHS Board for approval.

7.2 **Information Governance Committee meeting dates 2025/26**

Committee members received the meeting dates which had previously been circulated and approved by members via e-mail. There would be one in person meeting in May 2025.

Outcome: Committee members noted the meeting dates which had been approved by members via e-mail.

7.3 **Information Governance Operational Delivery Group**

Committee members noted the draft minutes of the group meeting held on 27 January 2025.

Dr McGuffie advised that the Head of Resilience at NHS Dumfries & Galloway would join the Area Clinical Forum meeting on 7 March 2025 to update on the impact of the cyberattack there. The presentation would be recorded and shared with Committee members for awareness. **CMcG/AO**

8. Key items to report to NHS Board

8.1 Committee members agreed that the following key issues be reported to the NHS Board meeting on 31 March 2025:

- Risk register – no changes to risk grading and no emerging risks.
- IG report, CRM update – request for report to have greater focus and context, including around areas of low compliance, risk and organisational impact.
- IGC ToR supported for onward submission to Board for approval.

9. Any Other Competent Business

9.1 There was no other business.

10. Date and Time of Next Meeting
Monday 12 May 2025 at 9.30am, Meeting Room 1, Eglinton House, Ailsa

Signed by the Chair, Marc Mazzucco Date: 12 May 2025