Approved by Committee on 24 February 2025

Information Governance Committee
Monday 11 November 2024 at 9.30am
MS Teams meeting

Present: Ms Sheila Cowan, Non-Executive Board Member (Vice Chair)
Mrs Jean Ford, Non-Executive Board Member
Mr Neil McAleese, 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 item 6.1
Ms Natali Higgins, Information Governance (IG) Manager, Corporate Records item 6.2
Ms Marie Lynch, Deputy Data Protection Officer item 6.2.3
Ms Tara Palmer, FOI Officer item 6.2
Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Welcome / Apologies for absence

1.1 The Vice Chair, Mrs Sheila Cowan, welcomed everyone to the meeting. The agenda was re-ordered slightly to allow colleagues providing updates to join the meeting.

1.2 Apologies were noted from Mr Marc Mazzucco, Cllr Douglas Reid and Ms Linda Semple.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 2 September 2024

3.1 The minute of the meeting held on 2 September 2024 was approved as an accurate record of the discussion.

4. Matters Arising

4.1 The action log had previously been circulated and members received an update on the following actions:

Item 8.1 (02/09/2024), Information Governance Operational Delivery Group (IGODG) – Due to diary conflicts, Dr McGuffie had not yet met with Mr Mazzucco. Dr McGuffie advised that as previously reported, the IG team continued to experience workforce challenges due to long term absence, staff turnover and increased

workload. The team had recently appointed an IG assurance officer to support Freedom of Information and Corporate Records Management work and an additional IG analyst. A recruitment process was ongoing for an interim Head of IG, with interviews taking place next week. Capacity and demand pressures meant that the IG team was taking a prioritised approach to ensure NHSAA met its legislatives duties and responsibilities, as well as the core work of the team.

The team had managed to re-establish the IGODG and draft minutes from the last meeting were provided with the meeting papers. The IG report to be discussed later in the meeting would take an asset based approach, focusing on work currently being done while categorising other areas that could not currently be progressed but did not impact on the legislative framework. Action complete.

Item 6.1 (29/04/2024), Cyber Security update – A paper had been submitted to the Strategic Digital Delivery Group and approved which would be shared with Committee members. Action complete. **NG/MD**

Item 7.1 (29/04/2024), NIS Audit – There had been slippage on the disaster recovery and business continuity testing exercise but this should be completed before end-December 2024.

Item 6.2.4 (29/04/2024), ICO audit action A04, review of policies and procedures – members noted the update and requested that the target completion date be reviewed and updated. **CMcG**

Item 5.2 (06/02/2024), IG update, Record of Processing Activities/Information Asset Register – members noted the update and requested that the target completion date be reviewed and updated. **CMcG**

4.2 **Information Governance Committee Work Plan 2024** – Committee members noted the work plan.

5. Risk

5.1 Information Governance Committee (IGC) Strategic Risk Register

The Medical Director, Dr Crawford McGuffie, presented the IGC Risk Register report. Following the recent Board workshop on Risk, this had highlighted the need for further review of risk reporting to the committees.

Dr McGuffie advised that all three IGC risks had been reviewed during the reporting period. Risk ID 603, service/business interruption – cyber incident remained high given the constant cyber risk. Risk ID 557, compliance – information governance, had been extensively reviewed and while the risk level had not changed, additional work had been done in relation to the risk matrix. For risk ID 856, COVID-19 Inquiries - retention of mail boxes, members

recognised the work done to mitigate the risk and approved that this be terminated and moved to the operational risk register.
Dr McGuffie confirmed in reply to a comment from a member that he would change the wording used from termination of risk to re-categorisation of risk across all risk reports to reflect that the risk continued to be managed at operational level.

There were no emerging risks to report.

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 and the Board's current performance against a number of national Cyber Security measures.

NHSAA was the first Scottish Board to complete the rollout of MS Baseline, which included Edge and Chrome policies, enabling Windows firewall and user access controls. Following a test of change to apply Baseline to a group of devices in the GP estate, there had been some challenges, primarily related to firewall and user access controls, due to the various software used. Work was taking place with the Infrastructure team to address areas of challenge.

Work was ongoing to remediate vulnerabilities detected during monthly scans. There was monthly reporting of vulnerabilities on the server estate. The Board would switch over to use of MS Defender antivirus over the next couple of years.

Work had begun alongside Trend Micro to migrate the current server estate to the New Vision One console. The Board had an ongoing contract with the National Cyber Security Centre and other external stakeholders to ensure the security of all external websites within the organisation, including GPs. The largest issues related to systems procured by the Health and Social Care Partnerships, with three different websites and each having different issues.

Mr Duggan updated that around 9,000 staff had completed cyber security awareness training following the move to Turas. There had been an issue with Learnpro not linking with Turas earlier in the year which had impacted on completion of this training, however, the position was expected to pick up before the end of October 2024. A communication would be issued to remind staff of the need to link

their Turas and Learnpro accounts. Four members of the cyber security team had taken advantage of Scottish Government funding to complete CompTIA Security+ training.

Mr Duggan clarified in reply to a question form a member that while Turas and Learnpro were linked, training uptake data was provided through Learnpro. Members requested that future reports provide details of cyber security training uptake as a proportion of the total number of staff to enable members to monitor compliance. **MD**

The Cyber Security team engaged with CoretoCloud alongside the Resilience team to provide Crisis Simulation training for the organisation which took place on 29 August 2024. The exercise was well received. While a number of staff found it focused towards IT, it had encouraged them to consider business continuity within their service area.

Cyber Month took place in October 2024 and this coincided with the launch of the new Cybersecurity SharePoint site. Communications were issued via Daily Digest and eNews similar to previous years covering malware protection; keeping smartphones/tablets safe; passwords; and phishing attacks.

NIS audit work continued as part of the three year cycle. The next two audit periods would focus on the 35 part or not achieved controls from the last audit in Spring 2024. While there had been slippage in relation to business continuity and disaster recovery, business continuity plan exercises should take place by end-December 2024, with disaster recovery taking place after that. Mr Duggan confirmed that going forward this would be done cyclically, at least on an annual basis. CoretoCloud and live testing of the Trakcare host environment should also reduce the number of controls not achieved. Further evidence was needed for the controls related to back-up and testing, specifically immutable back-up. The report provided an overview of likely compliance by the end of next year.

Committee members discussed and were assured by the level of activity taking place, commending in particular the significant work done to enable rollout of MS Baseline.

The Committee considered the level of detail provided in the report. The Chief Executive underlined that for all Governance Committees there was a need to take a balanced approach and provide the appropriate level of detail and assurance to enable members to deliver their governance and scrutiny role whilst not moving into the operational space. Following discussion, members agreed that the report should be reviewed and streamlined. Pending completion of the NIS audit action plan, further detail would be provided in the report's appendices to give members assurance of the controls in place and how they are working. Learning from this review work would be shared more widely for other Governance Committee reports going forward. **NG/DG/MD**

Approved by Committee on 24 February 2025

Outcome: Committee members noted the update on Cyber Security team activities over the reporting period. Members agreed that the report be reviewed and streamlined. Pending completion of the NIS audit, additional detail on NIS audit actions would be provided as an appendix to the report.

6.2 **Information Governance Work Programme 2024/25**

Committee members received an update outlining the current legislative and Board requirements which are required to be prioritised by the team at present to provide the Committee with insight into the current workloads.

6.2.1 **Corporate Records Management (CRM) update**

Ms Natali Higgins, IG Manager, Corporate Records, provided an assurance update on CRM and outlined priority work being progressed to ensure the Board complied with the requirements of the Public Records (Scotland) Act and other legislative requirements:

- Oversight of Directorate CRM improvement plans.
- Scottish Government had published a new Records Management Code of Practice and work was ongoing to ensure NHSAA's policies and guidelines are compliant, updated and relevant.
- Records retention and disposal policy and schedule – work was being progressed at pace to implement and ensure compliance with the Scottish Government records retention schedule.
- Priority work taking place to develop a central paper records storage area at Ailsa site – rationalisation of estate and move to distributed working had escalated the requirement for this to ensure records are stored properly.
- Ongoing support to COVID-19 Inquiries – to put processes, guidelines and communications in place to support teams to ensure they retain information that may be required as evidence.
- Management of employee records – guideline going through approval process and short messages for staff to support these records to be managed appropriately.
- Support for implementation of Office365 which will significantly improve the way records are stored and handled and how staff communicate and collaborate in the future. This significant work will support best practice in records management. Ongoing engagement and dialogue with the team in relation to guidelines, risk assessment and rollout of training to ensure records management elements are covered.
- The information asset register was being reviewed to support introduction of OneTrust although this work was being progressed with lower priority than the areas above.

6.2.2 **Information Commissioner's Office (ICO) Action Plan update**

As previously discussed, long term staff absence, workforce, demand and capacity issues had led to slippage in progressing the ICO action plan.

- For ICO Audit Action A04, the Controlled Document policy was still under review and had not yet been submitted for approval. A communications plan had been drafted and once the policy was published this work would progress.

- For ICO Audit Action A06, as previously reported this was a significant piece of work. Progress had been made by development of the IG Data Processing Agreement log and adoption of OneTrust. Once stability in the team's leadership had been restored and new team members were in their roles, the team would be able to progress actions.

6.2.3 **Data Protection (DP) update**

Ms Marie Lynch, IG Manager and Deputy Data Protection officer, provided the following update.

- As reported earlier, an IG analyst was recruited in September 2024 which should relieve pressure in relation to data protection activity.
- Certain areas were being prioritised to manage risk. Four Boards had received reprimands from the ICO in the last two years which highlighted the day to day importance of this aspect of IG work.
- Advice and guidance continued to be provided on complicated DP matters for all NHS staff and 53 GP practices, with queries often time sensitive.
- Significant increase in data rights requests, including subject access requests, with 23 requests so far this year. Some requests were sizeable and involved a significant amount of work, with a one calendar month statutory timeframe to respond.
- The team was responsible for investigating and responding to complaints and concerns related to processing of personal data by NHSAA and Ayrshire and Arran GP practices in accordance with the local complaints procedure.
- The team assessed new projects and changes to processes that involved processing of personal data, with the number of assessments completed consistently high. The assessment process was complex and often required a Data Protection Impact Assessment to identify DP risks and mitigations to reduce risks. There was currently a backlog of assessments awaiting approval due to resource issues in the team and a prioritised, risk based approach was being taken to complete this work.
- The team reviewed all requests for access to personal identifiable data for specific purposes and scrutinised requests for access to information systems to ensure compliance with

DP legislation and Caldicott principles. The team was also responsible for the FairWarning system in NHSAA to identify inappropriate access to patient information held on the Board's clinical systems and progress via HR where appropriate.

- The team was responsible for reviewing all IG related adverse events on Datix, identifying actions required and providing advice and guidance to reviewer. To report any breaches that meet criteria to ICO.
- Information security breaches for the period July to September 2024 were outlined in Appendix 1. There were a total of 41 breaches reported from across the organisation during the reporting period, greater than the average number over the last three years. Ms Lynch advised that this could reflect better reporting rather than an increase in breaches as the number reported was low given the size of the organisation. Ms Lynch confirmed that following the personal data breach reported to ICO, the department had looked at processes and was currently updating these, with wider learning to be shared across the organisation.

6.2.4 **Freedom of Information (FOI) update**

Ms Tara Palmer, FOI Officer, highlighted the following areas:

- Following a slight decrease in requests reported at the last meeting, there had been 123 requests received in October 2024. FOI requests were sitting at 0.8% behind the same point last year, which was the busiest year ever, however, this was 27% higher than the same point in 2022.
- The Board was currently achieving 91.4% compliance in responding to requests within 20 working days, with slightly reduced performance compared to the last five years.
- The Board had one FOI officer responsible for responding to all requests. Since August 2024, the new IG Assurance Officer had been providing 0.5 WTE FOI support, with additional ad hoc support provided by the IG Analysts when required. However, given the number of FOI requests received, the complexity of requests and time taken to respond working with services, the position was challenging, even with the additional resource being provided. This meant that there was no capacity to take on other tasks at this time.
- Should Boards fail to meet the requirements and standards set out in FOI legislation, the Scottish Information Commissioner could carry out interventions with Boards. While NHSAA was not at intervention point, significant time and effort was required to manage FOI requests to maintain compliance and avoid intervention.

Ms Palmer advised in reply to a question from a member that while the majority of FOI requests were from the public, around 30% of requests came from MP and MSP offices. The Medical Director, Dr Crawford McGuffie, advised that discussion had taken place with West of Scotland Medical Directors and all six Boards had reported a

similar position. Dr McGuffie would draft a letter to local MPs and MSPs to highlight some of the pressures facing the Board and the impact of current FOI demands. **CMcG**

Members discussed the report and acknowledged the workforce, demand and capacity pressures facing the IG team. Dr McGuffie reassured members that a prioritised approach was being taken to ensure the Board met legislative requirements and the risk related to IG resources continued to be managed at operational level.

Outcome: Members received the IG report and took assurance from the work being done to promote compliance with Data Protection Legislation. The Committee thanked the IG team for the good work being done with limited resource.

7. Corporate Governance

7.1 Information Governance Operational Delivery Group (IGODG)

Committee members noted the draft minutes of the IGODG meeting held on 21 October 2024.

8. Key issues to report to NHS Board

8.1 Committee members agreed that the following key issues be reported to the NHS Board meeting on 2 December 2024:

- Strategic risk register – assurance of work being done to mitigate risk and re-categorisation of Risk ID 856, COVID-19 Inquiries – retention of mail boxes to operational risk register.
- Cyber security progress update and rollout of MS Baseline in NHSAA.
- IG team workforce pressures – assurance of work being done and prioritised approach being taken to manage risk and meet legislative requirements.

9. Any Other Competent Business

9.1 There was no other business.

10. Date and Time of Next Meeting

Monday 24 February 2025 at 9.30am, MS Teams meeting

Signed by the Vice Chair, Mrs Sheila Cowan Date: 24 February 2025