Approved by Committee on 2 September 2024

Information Governance Committee
Monday 29 April 2024 at 9.30am
Room 1, Eglinton House, Ailsa Hospital, Ayr

Present:	Mr Marc Mazzucco, Non-Executive Board Member (Chair) Ms Sheila Cowan, Non-Executive Board Member Mrs Jean Ford, Non-Executive Board Member (joined via MSTeams)
Ex-officio:	Ms Claire Burden, Chief Executive and Senior Information Risk Owner Mrs Nicola Graham, Director Infrastructure and Support Services
In attendance:	Mr Martin Duggan, Cyber Security Manager Item 7.1 Mr Derek Gemmell, Assistant Director, Digital Services Item 6.1 Ms Debbie McCard, Risk Manager Item 5.1 Ms Ann Catherine Wilson, Head of Information Governance (IG) Items 6.2 and 8.2 Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Apologies for absence

Apologies were noted from Mrs Lesley Bowie, Cllr Douglas Reid and Dr Crawford McGuffie.

2. Declaration of any Conflicts of Interest

There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 26 February 2024

The minute of the meeting held on 26 February 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.

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

5. Risk

5.1 **Information Governance Strategic Risk Register**

The Risk Manager, Ms Debbie McCard, presented the Risk Register report. The report had been discussed in detail at the Risk and Resilience Scrutiny and Assurance Group (RARSAG) meeting on 19 April 2024.

Ms McCard advised that the report's format had been amended

following feedback from Governance Committees, with more detail on control measures and ambitions for risk set out in the report.

During this reporting cycle there were three Information Governance strategic risks. Two risks had been reviewed, with no change to the risk rating. Further detail had been added to risk ID603, Cyber Security, related to cyber risk following the cyberattack at NHS Dumfries & Galloway (NHSDG).

The Chief Executive, Ms Claire Burden, confirmed in reply to a query from a member about risk ID603, that she was content for the risk grading to remain as high. Mr Gemmell confirmed that RARSAG would consider if some of the recommendations from the NHSDG cyberattack should be added as mitigations to risk ID603.

For risk ID 856, Adverse publicity/reputation, COVID-19 inquiry, retention of mail boxes, currently being tolerated, audit work was ongoing and an update on the functionality of the additional controls should be provided by 30 April 2024. The Director of Infrastructure and Support Services, Mrs Nicola Graham, clarified in response to a question from a member that less than 10 email boxes had not been retained prior to the action to retain mail boxes of key decision makers above Grade 8a who had left the organisation.

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

The Assistant Director, Digital Services, Mr Derek Gemmell, provided an update on key areas of activity undertaken by the Cyber Security team during the period January to March 2024. The following areas were highlighted:

- Work continued with Bitlocker encryption on laptops.
- The whole desktop estate had now moved to MS Defender AV, to provide better security and give centralised reporting to the NHS Scotland Cyber Security Operations Centre (SOC).
- AV detection – work continued to monitor vulnerabilities and malicious activity, with nothing specific to flag to members.
- There were continued very low levels of suspicious activity and alerts from the SOC.
- Successful pilot work had taken place to implement MS Security Baseline. Following the successful pilot this should be applied to the full estate from May 2024. Mr Gemmell advised in reply to a query from a member that this software would

provide better security around the use of personal devices, in line with the Board's information governance policy. The Board's IT service desk would be able to help individuals should they have any access issues.

- Over 7,500 staff had completed the Cyber Security Turas Learnpro between October 2023 and March 2024. This training continued to be publicised through eNews and other means to ensure all staff complete as part of their mandatory training.
- Network and Information Systems (NIS) Audit 2023/24 – the audit was completed in February 2024 and the outcomes would be discussed later in the meeting.
- Internal Cyber Security and Resilience Audit – the current internal auditor, Grant Thornton, had compiled the final management report of the 2023 internal audit. The Board continued to work on the advisory actions raised, with papers scheduled for the Strategic Digital Delivery Group in June 2024 to close off remaining actions.
- An SBAR report had previously been circulated to Committee members on the cyber security incident at NHS Dumfries & Galloway (NHSDG) and NHS Ayrshire and Arran's (NHSAA) response. Mr Gemmell gave assurance that it was unlikely that a similar situation could arise in NHSAA due to systems and processes in place locally. Considerable work had been done working with national teams and guidance had been identified and mitigations were being put in place.

Committee members discussed the two areas of compliance identified through National Shared Services recommendations following the recent cyberattack at NHSDG. The Chief Executive reassured members that work was ongoing, including identification of funding for a National Cyber Security Centre accredited cyber incident response provider.

Outcome: Committee members noted the summary of the Cyber Security team activities over the reporting period. Members received assurance on the work being done and mitigations in place following the cyber security incident at NHS Dumfries & Galloway.

6.2 **Information Governance Update report**

6.2.1 The Head of IG, Ms Ann Catherine Wilson, provided a presentation on OneTrust and highlighted the following key areas:

- Record of Processing Activity (ROPA) – under Article 30 of Data Protection legislation it is a minimum legal requirement for Boards to have a ROPA for processing healthcare activity, including whose information is held and who this is shared with. NHSAA's ROPA is held on OneTrust.
- Information Asset Register (IAR) – Ms Wilson explained that while it is good practice for the organisation to have this, as it

shows how information is held and protected, there is no legal requirement for this.

- The Board's ROPA linked to multiple assets and processing activities, for example, patient records, finance and human resources and this would continue to be added to.
- Members received an overview of the OneTrust dashboard.
- Ms Wilson clarified in reply to a query from a member that OneTrust did not include equality characteristics as this did not fall under the Board's IG role, however, this information could be added if required.
- Ms Wilson advised that work to input information to OneTrust was at an early stage and would continue to progress, although it had had been impacted by staffing issues and the need to meet other priorities and statutory deadlines. The early progress made and sustainable approach being adopted was noted during the recent ICO audit, with no concerns raised following the audit.
- OneTrust could also be used to produce data protection impact assessments (DPIA). Consideration was being given to using IG checklists and templates to make this process easier although staff would need to be trained to use the system. The data processing and sharing tracker previously developed would be reviewed and updated to allow progress to be monitored and to ensure information held was up-to-date.
- Locally, documentation was being developed to allow the user to quickly assess if information meets Article 30 requirements.
- A working group had been set up nationally to look at sharing good practice in the use of OneTrust.
- Following the UK's exit from the EU, the UK had adopted the General Data Protection Requirements (GDPR) and an Adequacy Agreement was agreed up to 2025, to allow information to be shared with EU countries. Should significant changes be made to the Bill that was previously agreed, the UK would become a third country and would have to ensure other standard contract clauses in the transfer to assure that IG Standards were the same.

Ms Wilson advised in reply to a query from a member that she did not envisage significant opportunities for financial savings through the use of OneTrust for DPIA, with tracker information currently held by the team being moved across to OneTrust to monitor progress. She explained that the national contract for OneTrust ran on a yearly basis. Under procurement law the contract required to go out to tender so it may not be OneTrust but a similar system being used in the future. Ms Wilson reassured that colleagues involved in this process at national level recognised the importance of the information currently held on OneTrust being transferable to another system.

Committee members acknowledged the progress made to date. Members were encouraged that details of assets and processing activities would be held in one central repository, with the ability to monitor and track progress. Members discussed the national contract and reiterated the importance of being able to transfer information

from OneTrust to any new system.

Committee members requested a more detailed update on progress to date and the timescale for completion of work to transfer assets and processing activities to OneTrust at the next meeting. **CMcG/AW**

6.2.2 **Information Security Incident report**

The Head of IG, Ms Ann Catherine Wilson, presented the information security incident report. There were two breaches reported to the Information Commissioner's Office (ICO) and one case was being investigated by the ICO related to a subject access request which had gone through another department and had not been recognised. The team involved would undergo training to prevent any recurrence. Ms Wilson reassured members that this had been an isolated incident.

6.2.3 **Information Governance (IG) Work Programme**

The Head of IG, Ms Ann Catherine Wilson, provided a verbal update on progress with the following actions on the IG work programme, noting that some actions could not be progressed due to delays at national level:

- **Public Records (Scotland) Act (PRSA) 2011, Action 7, Archive and transfer** – Feedback was still awaited from South Ayrshire Council related to charges for storing and archiving of material.
- **PRSA, Action 11, Audit Trail** – this Element would remain at Amber until Sharepoint was implemented.
- **PRSA, Action 15, Public records held or created by third parties** – Some progress had been made and a contract clause had been included in generic terms and conditions. Work continued in other areas still marked as Amber.
- **Freedom of Information (Scotland) Act 2022 (FOI)** – good progress had been made with FOI training and this action was now marked Green, with positive feedback on training and changes made.
- **Microsoft 365 implementation** – Funding was now in place for a national resource to lead this work on a Once for Scotland basis, although local support would still be required to bring this work to fruition.

  The Director of Infrastructure and Support Services, Ms Nicola Graham, advised in reply to a query from a member that M365 had to be implemented quickly in response to the COVID-19 pandemic and some elements of the rollout were having to be done retrospectively which was challenging as people were already using the system. She highlighted the work ongoing at national level to bring the different elements of IT together, including security aspects. Sharepoint could not be rolled out nationally until this work was complete. Ms Wilson reassured that the IG team had worked closely with the Cyber Security team to put in place applications locally and ensure these met local

governance around acceptable use standards. She reiterated that further work was required at national level in relation to higher level functionality.

The Committee discussed the update provided and were assured of the activity taking place locally to progress local work as far as possible, and that other actions were being discussed in detail at national level. Committee members requested regular assurance reports detailing progress with the IG action plan, including appropriate timescales, to enable members to monitor actions to completion. **CMcG/JW**

6.2.4 **Information Commissioner's Office audit report action plan**

The Head of IG, Ms Ann Catherine Wilson, provided a verbal update on progress with the three actions outstanding:

- **A04, review of policies and procedures** - on hold. Ms Wilson explained that this action did not sit solely with the IG team and wider discussion was required around the process for approving all policies and procedures across the organisation. Ms Wilson would discuss with other parties involved and agree a target completion date, with progress to be reported at the next meeting. **AW**
- **A06, ensuring all processors comply with the terms of written contracts** – This action involved significant work and had been partially completed. A contract variation notice had been sent to contractors. Discussion was ongoing with the Procurement team which had submitted a successful request for additional staff to support the procurement function, to work together with the IG team to ensure contracts are compliant.
- **A09, detailed data sharing agreements to meet legislative requirements** – this action had been completed.

The Chief Executive, Ms Claire Burden, acknowledged the challenges in completing some of these actions and recognised that progress had been made in taking forward high priority areas. Many of these projects were continuous and there was no end completion date, with progress being reported through the Corporate Management Team. The Chief Executive emphasised that the Committee should receive regular assurance reports on progress being made and next steps, including any interdependencies and links to other services in terms of delivering compliance.

Ms Wilson would provide a detailed update at the next meeting with a breakdown of actions being taken, progress made and next steps. **CMcG/AW**

6.2.5 **Information Asset Register**

Please see item 6.2.1 above.

Outcome: Committee members noted the IG update.

7. Audit

7.1 **Network and Information Systems (NIS) Audit**

The Head of IT Security, Mr Martin Duggan, provided a detailed presentation to update on the results of the NIS audit and highlighted the following areas:

- Outlined background to NIS audit, a three-year programme of audits and reviews of Boards to evaluate compliance with the NIS regulations. First three year cycle completed in 2022.
- First full audit of second three-year cycle carried out in 2023/24 showed NHSAA's overall compliance at 87%.
- Auditors had commented on the Board's strong submission, positive approach to contingency planning and close working with the IG team.
- Mr Duggan outlined areas where compliance was achieved and areas requiring further work to achieve full compliance.
- There were 14 categories and 53 sub categories with over 80% compliance, and 10 over 90%.
- All 17 categories and 61 sub categories achieved the target of 60% or above.
- One sub-category was below 30% and focused work would take place related to business continuity plans and disaster recovery testing.
- There were no categories with zero compliance.
- Next evidence submission date is 5 February 2025.

Committee members welcomed the report and the positive feedback provided by the auditors. The Committee requested that six monthly assurance reports be provided going forward to give greater visibility in relation to controls partly achieved or not achieved and work planned, with timescales, to allow members to monitor progress to completion. **NG**

Outcome: Committee members note the summary of the NIS audit 2023/24 final report. Members looked forward to receiving a detailed report outlining progress with areas either partly or not achieved at the meeting in November 2024.

8. Corporate Governance

8.1 **Information Governance Committee Annual Report 2023-2024**

The Committee Chair, Mr Marc Mazzucco, presented the draft annual report setting out the Committee's key achievements during the year in delivering its remit.

Outcome: Committee members approved the annual report, self-assessment checklist, assurance mapping report and assurance of reporting to the NHS Board for onward submission to the NHS Board.

Approved by Committee on 2 September 2024

8.2 **Information Governance Operational Delivery Group**

Ms Wilson advised that as the group meeting scheduled for 22 April 2024 was cancelled there was nothing to report.

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 21 May 2024:

- **Cyber security –** NHSDG cyberattack and mitigations in place locally to prevent cyber incident.
- **Information Governance** - Future reporting arrangements for IG work programme.
- **NIS audit report -** progress made and action plan to be developed.
- **IGC annual report 2023-2024** – approved for onward submission to the NHS Board on 21 May 2024.

10. Any Other Competent Business

10.1 There was no other business.

11. Date and Time of Next Meeting
Monday 2 September 2024 at 9.30am, MS Teams

Signed by the Chair: Marc Mazzucco Date: 2 September 2024