Approved by Committee on 17 November 2025

NHS Ayrshire & Arran

Information Governance Committee
Monday 1 September 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 Sharon Morrow, Non-Executive Board Member
Cllr Douglas Reid, Non-Executive Board Member joined at item 5.1

Ex-officio: Prof Gordon James, interim Chief Executive and Senior Information Risk Owner
Mrs Nicola Graham, Director of Infrastructure and Support Services
Dr Crawford McGuffie, Medical Director, Caldicott Guardian
Ms Marie Lynch, interim Head of Information Governance and Data Protection Officer (DPO)

In attendance: Mr Martin Duggan, Cyber Security Manager item 6.1
Ms Tara Palmer, Freedom of Information Officer item 6.2.3
Mrs Angela O'Mahony, Committee Secretary (Minutes)

1. Apologies for absence

1.1 Apologies were noted from Mrs Lesley Bowie, Mrs Jean Ford and Ms Marie Richmond.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 12 May 2025

The minute of the meeting held on 12 May 2025 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, ICO Audit action A04, review of policies and procedures – The Controlled document policy was currently under review and being amended by the Chief Executive's office. The revised policy will focus on the framework for policy management required to deliver good governance as part of systems of internal control. Workforce resource issues in the Corporate Governance (CG) team have impacted on the progress of this action. To mitigate the risk, the Information Governance (IG) team will work with the CG team to get the policy completed in the next few months.

Item 6.2.4, ICO audit report action plan – Ann Wilson had now retired from NHSAA and Marie Lynch had taken on the role of interim Head of IG and Data Protection Officer. Marie Lynch had provided an update on the Register of Processing Activity (ROPA) at the last meeting, advising that the OneTrust national contract had ended and that NHSAA was considering use of M365 functionality to provide a ROPA as part of its implementation. In progress.

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

5. Risk

5.1 Information Governance Strategic Risk Register

The Medical Director, Dr Crawford McGuffie, presented the Risk Register report. The report had been discussed in detail at the Risk and Resilience Assurance Group (RARSAG) meeting on 18 July 2025.

The Director advised that both strategic risks related to the Information Governance Committee (IGC) had been reviewed during this reporting period with no change to the risk ratings. There were no risks for escalation or termination.

Following discussion at the last IGC meeting around risk scoring for Risk ID 557, compliance – information governance, the risk was currently being reviewed with a plan to develop individual risks for Corporate Records Management, Freedom of Information and Data Protection. Once the individual risks have been developed this will allow each risk to be re-assessed in relation to the current risk scoring and positioning on the appropriate risk register. Committee members discussed and supported this approach.

Members highlighted discussion at the last meeting around likelihood and consequence and the need to clarify target dates aligned to risks. Members looked forward to receiving outputs from the short life working group set up to consider future risk reporting.

The Director of Infrastructure and Support Services, Nicola Graham, advised in reply to a question from a member that Risk ID 603, Cyber Incident, that the consequence of a cyber incident would be severe and the level of risk would not change regardless of mitigations. As had been discussed previously, the likelihood score had not changed as threats and therefore mitigations changed continually. The key was to keep the Board's knowledge current and for mitigations to change in response to emerging threats. The risk was due for review by 30 September 2025 and as part of the review, the team would reach out to other West of Scotland Boards to seek information on cyber incident risk ratings for comparison. The Director advised that the Board would undergo a cyber security internal audit in the near future and scoping for the audit is currently being agreed. The audit

recommendations would be shared with the Committee later in the year and should provide an additional level of assurance to members.

The Chief Executive, Gordon James, advised that NHSAA was at the forefront of the roll-out of M365 and MS Defender which put the Board's cyber security in a stronger position than some other Boards. NHSAA had received positive feedback following the Network and Information Systems audit, which achieved above some thresholds and was performing well in comparison with other Board areas.

The interim Head of IG, Marie Lynch, advised in reply to a question from a member that due to staffing constraints, the IG team was focusing on delivering legislative requirements which had led to a delay in the completion of some other actions, for example, implementation of a training calendar. This was being looked at as part of the ongoing IG internal audit and should be completed by the next Committee meeting.

Dr McGuffie advised that further discussion would take place on the above risks at the Information Governance Operational Delivery Group and Risk and Resilience Scrutiny and Assurance Group and an update would be provided at the next Committee meeting on 17 November 2025.

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 Director of Infrastructure and Support Services, Nicola Graham, introduced and invited Martin Duggan, Cyber Security Manager, to update on key areas of activity undertaken by the Cyber Security team. The following areas were highlighted:

- Members received assurance that the team was taking reasonable precautions to mitigate cyber security risks within the organisation.
- The team continued to improve cyber exposure scores and strengthen security, with a resolution rate of 97.4% of calls raised.
- There had been a small increase in malware detected due to a particular strain affecting a small number of devices. Key performance indicator data was provided in the report related to malware incidents.

- The team remained vigilant to risks, threats and vulnerabilities in the wild, focusing on the top 50 vulnerabilities and these were reducing each quarter.
- Members received a detailed presentation on the findings and recommendations following a phishing simulation carried out in conjunction with the NHS Security Operations Centre in May 2025. 6% of staff clicked the "malicious" link with a quarter of those having provided credentials which was of concern. An improvement plan had been developed and the individuals who had clicked the link were asked to complete Cyber Security training within 30 days. Staff who had not yet completed this training had been contacted again. Should they fail to respond the issue would be raised through the line manager. Newsletters would be sent via Communications team on four cyber security topics to raise awareness. Cyber Security month in October 2025 would also address these topics. Consideration was being given to future staff communication to highlight the importance of cyber security.
- A second phishing simulation was planned for November 2025, with the aim to reduce by half the number of staff who click the link and provide credentials. Phishing simulations would continue on a six-monthly basis. There were plans to collate information on those who click "malicious" links at Directorate level to enable targeted education and improvement work to take place.

The Medical Director, Dr Crawford McGuffie, was encouraged by the work being done by the team, the supportive educative mechanisms in place and progress to reduce risk.

Committee members emphasised the importance of staff completing Cyber Security training given the cyber risk to the organisation and potential negative impact on patient experience. Members considered approaches to encourage staff uptake of this training. Martin Duggan clarified that Cyber Security training has to be completed by staff every two years as part of mandatory and statutory training, with the same training module used by a number of other Boards.

In reply to a question from a member, Martin Duggan advised that good progress was being made in upgrading devices to Windows 11 following a phased approach and he had no major issues or concerns to highlight at this stage.

The Executive team would consider how to increase uptake of Cyber Security training further out with the meeting and report back at a future meeting. **NG**

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

6.2 **Information Governance Update report**

Committee members received a combined Information Governance update on the Board's obligations in relation to Information Governance.

6.2.1 **Information Security Incident Report**

The interim Head of IG and DPO, Marie Lynch, advised that there were 26 breaches during the reporting period which was slightly higher than the quarterly average.

During the quarter April to June 2025, there was one data breach considered to be notifiable to the Information Commissioner's Office (ICO). This data breach related to inappropriate access to information and was currently under investigation locally, with progress to be reported to ICO. A stop press had been sent to remind staff of the Fair Warning system. The team was currently looking at refining Fair Warning reports, working with Digital and Health Records, to review access controls for clinical systems to ensure appropriate role based access to patient information to deliver safe patient care whilst adhering to Data Protection and Caldicott obligations.

The majority of breaches were within Acute services which was to be expected given the size of the Directorate. Most breaches were categorised as Caldicott and Data Protection, consistent with previous quarterly reports. All breaches were handled in line with the procedure for reporting and managing information security breaches. All remedial actions had been taken and lessons learned had been shared as required. The team was continually working to highlight the need to report breaches and a section on data protection had been included in risk management training to raise staff awareness that these breaches constitute an adverse event.

During the reporting period, the ICO reviewed no complaints related to NHSAA processing personal data.

6.2.2 **Public Records (Scotland) Act (PRSA) annual update (Corporate Records)**

The interim Head of IG and DPO, Marie Lynch, advised that the Corporate Records Manager, Natali Higgins, had left NHSAA to take up a promoted post within the National Shared Services M365 team and a recruitment process was ongoing.

Marie Lynch provided a detailed update on progress with the Records Management Plan (RMP) to improve management of corporate records. The report outlined evidence to support compliance with 15 elements. There were no red elements. Members received a detailed update on the three amber elements:

Element 4, business classification scheme;

Element 11, audit trail; and

Element 15, public records created or held by third parties.

The remaining elements were green.

Members received an update on Directorate Improvement Plans developed and implemented in October 2023. Directorates were required to undertake 66 actions split into 10 requirement areas, with quarterly updates to allow monitoring and reporting. The report provided details of current completion rates, with the reporting year running from October to October. Marie Lynch highlighted areas of specific concern, including Pharmacy, Acute, People and Safety and NA and EA HSCPs.

Dr McGuffie advised that progress was being reported to Corporate Management Team and a continuous improvement approach adopted using data available, following up with areas that have not responded. Dr McGuffie had met all three Chief Officers and follow-up meetings had been arranged to discuss performance and challenges. Acute services were on an improvement trajectory. The Director would also meet with Pharmacy to discuss progress. In addition to Directorate improvement plans, significant work is taking place to ensure appropriate measures are in place to implement good records management across Ayrshire and Arran.

Marie Lynch advised that the Board had last completed a progress update review (PUR) in 2023 which noted that NHSAA continued to take its statutory obligations seriously and was working hard to bring all elements of records management arrangements into full compliance with the Act and fulfil the Keeper's recommendations. The Board had been invited to submit an updated PUR in August 2024, however, this had moved to biennial reporting with a report due for 2025/26. In response to a question from a member around the need to evidence continual improvement, Marie Lynch advised that the team did not currently have the resources to complete a 2024/25 PUR and this would be considered once the new CRM Manager is in post. **CMcG/ML**

Outcome: Committee members noted the PRSA update.

6.2.3 **Freedom of Information (Scotland) (FOISA) and Environmental Information (Scotland) Regulations 2004 (EIRs) update**

Tara Palmer, FOI Officer, provided the six-monthly FOI activity report highlighting the Board's obligations and compliance with FOISA and EiRs.

As reported previously, there continued to be a rise in FOI requests compared to the same period over the last two years. The continued volume of requests, increasing complexity and volume of questions, as well as organisational pressures, had impacted on compliance in responding to requests, which dropped from 91% in 2024 to 89.9% in

the first six months of this year. Acute services continued to receive the majority of FOI requests due to the size of the Directorate. MSPs continued to be the largest group making FOI requests. The team continued to work with Directorates to improve response times. The level of FOI requests and Board's compliance in responding was comparable to most other Board areas.

Members were advised that as part of the Office of the Scottish Information Commissioner's (OSIC) duty they could carry out interventions against authorities not complying with FOI law, with two Boards currently under level 3 intervention, as detailed in the report.

Tara Palmer advised that a decision was issued by OSIC in July 2025 for an appeal they had notified to the Board in April 2025. This related to a complex request which was not originally treated as a FOI. The Board therefore required to provide the applicant with a review under FOISA, with a response required by 5 September 2025.

There were five requests for internal review during the reporting period and all were responded to within the statutory 20 working days.

The Medical Director, Dr Crawford McGuffie, advised in reply to a question from a member that he had previously written to all MPs and MSPs about the volume of FOI requests being made, particularly by MSPs, and the pressures facing the team. This continued to be raised at quarterly meetings with MPs and MSPs. The Chief Executive, Gordon James, advised that once regular MP and MSP meetings have been set up he will continue to raise the issue. He highlighted that the issue was also being discussed with Scottish Government policy teams.

Outcome: Committee members noted the FOISA and EIRs six-monthly update.

6.2.4 **IG work programme update**

The interim Head of IG and DPO, Marie Lynch, provided an update on the IG work programme 2025/26. The following areas were highlighted:

- PRSA:
    - An update was provided earlier in the meeting related to Elements 4, 11 and 15.
    - Element 6, destruction arrangements was ongoing and this action would remain amber. Health Records already had robust arrangements in place.
- FOISA:
    - FOI training – ongoing to enable support to be provided to FOI Officer when required.
- M365 implementation:
    - The IG team continued to support implementation. Although resource is now in place nationally to support this action, no new national compliance documents have been

produced and the team continues to support the local M365 project team with documentation. This action will remain amber as ongoing.

- ICO Audit action A04, Policies and Procedures – as discussed earlier, the Controlled Document policy was still being reviewed by the CG team and it was hoped to have this approved in the next few months. A communication plan had been drafted and was ready to be implemented once the policy was approved.
- ICO Audit Action A06, Organisation's responsibility to ensure all processors comply with terms of written contract(s) – this action involved significant input from IG and Procurement. Due to resource issues within the IG team and the need to focus on delivering legislative requirements, this has not been able to be progressed further. The team had updated the processing log used for all DP agreements and this had been discussed with the Assistant Director, Digital Services. A meeting was planned to consider work that could be done together on an action from the NIS audit related to supplier management.

Outcome: Committee members noted the update on the IG work programme 2025/26.

7. Corporate Governance

7.1 Information Governance Operational Delivery Group

Committee members noted the draft minutes of the group meeting held on 21 July and approved minutes of the meeting held on 28 April 2025.

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 6 October 2025:

- IG strategic risk register – review of Risk ID 557 – Information Governance – proposal to split into three areas.
- Cyber security – phishing simulation – improvement actions. Cyber security training – how to improve staff uptake.

9. Any Other Competent Business

9.1 **Walkround to IG team** – Sharon Morrow, Non-Executive Board Member, advised that she had recently made a quality and safety walkround to the IG team. This had been an informative visit which had provided the opportunity to ask questions and learn more about successful work being done, as well as areas of challenge. In reply to questions from members, the Medical Director, Dr Crawford McGuffie, acknowledged the workforce resource issues facing the team over the last year and a half and thanked the team for their hard work during this challenging period. The Director advised that recruitment plans are now in place for a new Head of IG and DPO and Corporate

Records Manager. The Committee would continue to monitor progress.

10. Date and Time of Next Meeting
Monday 17 November 2025 at 9.30am, MS Teams meeting

Approved by the Chair, Marc Mazzucco Date: 17 November 2025