Approved by Committee on 25 August 2026

Information Governance Committee
Monday 18th May 2025 at 9.30am
Board Room, Ayr Hospital

Present: Mr Marc Mazzucco, Non-Executive Board Member (Chair)
Mrs Jean Ford, Non-Executive Board Member
Mrs Sharon Morrow, Non-Executive Board Member
Cllr Douglas Reid, Non-Executive Board Member

Ex-officio: Mrs Nicola Graham, Director Infrastructure and Support Services
Dr Crawford McGuffie, Medical Director, Caldicott Guardian and Senior Information Risk Owner

In attendance: Mr Martin Duggan, Cyber Security Manager
Ms Marie Lynch, Head of Information Governance
Mrs Eleanor Sands, Committee Secretary (minutes)

1. Apologies for absence

1.1 Apologies were noted from Prof Gordon James, Mrs Lesley Bowie and Ms Sheila Cowan.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 23 February 2026

The minute of the meeting held on 23 February 2026 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 were noted. Committee members received an update on the following actions:

Item 6.1 PR Scotland Act Update: The Chair discussed the update from East Ayrshire Health and Social Care Partnership. Contact has now been made with the Partnership, however, the action will remain "in progress" until the Corporate Records Improvement Plan Quarter 3 submission is received. Subject to receipt of that submission, the action may be considered complete at the next meeting.

4.2 **IGC Work Plan 2026** – 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 for discussion.

Following the Integrated Governance Committee meeting on 17 February 2026, it was agreed that a single strategic risk would be developed as a benchmark for good practice. This was supported by the Non-Executive Directors and is detailed in Appendix 2.

A programme of workshops and educational sessions have now commenced, alongside practical support from the Risk Management Team. It is anticipated that all strategic risks will be fully revised by July 2026.

There were four strategic risks aligned to the Information Governance Committee:

- Four were due for review.
- Four were reviewed with no movement on the scores.
- Freedom of Information and Corporate Records Management risks are expected to reduce for the next report.
- Data Protection will remain a risk.

Ms Jean Ford noted that, based on information shared with Non-Executive Directors, the organisation appears to have effective controls in place that may help reduce risk scores over time. Positive audit outcomes, along with the absence of breaches or concerning trends, should also be considered when reviewing those scores. The Committee noted that work would continue to support more realistic risk scoring, with potential benefits beyond Information Governance.

In response to a query from the Chair regarding whether this section would be redrafted, Ms Ford confirmed that it would be presented in the new reporting format and that the review process would continue until July 2026.

A committee member asked whether the cyber security risk relating to disruption of the surgical robot, including any impact on patient data or waiting times, should be treated as a strategic or operational risk. It was noted that this was not currently reflected in the report and that the cyber security risk and mitigating controls should form part of the assessment.
Mr Martin Duggan, Cyber Security Manager, advised that the supplier had been unable to access the surgical robot and as a result, patient waiting times might not be affected. The Committee noted that this should be reflected more clearly in the systems and impact assessment.

Ms Marie Lynch asked whether the Freedom of Information risk could change from strategic to operational, noting that the rating had remained positive, the Information Governance Assurance Officer was

now in post, and the risk appeared stable.
The Chair advised that the risk should remain unchanged at this stage, particularly as the Assurance Officer had only recently taken up the post. It was agreed that the matter could be reviewed again at a future meeting.

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 highlighted the following key areas of activity:

The paper is being presented to the committee for awareness:

NHSA&A continue to have robust cyber security measures in place within the organisation.

- Cyber Security MAST compliance fell to 53% in the previous quarter following the introduction of the new Once for Scotland module. Discussions are ongoing with the Training Centre, Ayrshire Central Hospital. Compliance levels are now beginning to recover and are expected to continue increasing over the coming year.
- The report highlighted the ongoing risk posed by suppliers and third-party supply chains. Two key supplier incidents were noted: Stryker experienced a cyber security incident affecting its Microsoft 365 network and remained offline for a period, however, there was no significant impact on NHS Ayrshire and Arran. Intuitive Surgical also experienced a third-party cyber security incident, which had no impact on NHS Ayrshire and Arran.
- Members received a summary of ongoing projects and improvements within the Cyber security team including:

    - Server vulnerability figures continue to decline.
    - The exposure score remains stable as a result of ongoing updates.
    - Although there have been a small number of malware spikes, there is no current risk to the organisation due to continual testing by the Cyber Security team.
    - The completion of incidents within the team is currently at 97% compliance.

- The upskilling fund to support ongoing training and development across the team has been secured once again.
- Work is progressing on anti-ransomware software implementation.
- The Windows Defender Application Control process is ongoing and is providing an improved level of assurance.
- Secure emails within Care Homes is in progress within the organisation.

Members also noted the Scottish Government 360 Assurance programme, which will replace NIS, with all testing and assessments completed by the March deadline.

The Internal audit is ongoing with an action plan in place, one action has already been signed off and currently working on others.

Mr Martin Duggan replied to a question regarding clarification on the timescale for improving the Defender Exposure Score and the device score, both of which are currently below the KPI. Mr Duggan advised that the Defender Exposure Score had previously been at KPI level, but the introduction of additional Microsoft controls has extended the time required for the score to reduce. It was explained that further tooling is being introduced to support improvement and also noted that the Secure Score is being affected by the rollout of new Microsoft controls, which has made it more challenging to maintain. It was anticipated that both measures would show improvement by the next Information Governance Committee meeting.

In response to a query from the Chair regarding the low training compliance rate, Mr Martin Duggan advised that the Training Centre had decided not to reset all staff compliance to zero. Instead, staff would be required to complete the module on an annual basis, which should lead to a gradual improvement in compliance figures over time and all staff should have completed the new module by March 2027.
Ms Nicola Graham added that training compliance is a wider concern across the new Once for Scotland modules and advised that this would be raised at the next Corporate Management Team meeting for action

In response to concerns raised about supply chain companies that may not have cyber security arrangements as robust as those in place within NHS Ayrshire and Arran, Ms Nicola Graham advised that suppliers with access to government systems are subject to strict controls. Ms Graham also advised that the Scottish Government is considering legislation that would make it unlawful for public sector bodies to pay ransomware to become less of a target.

NIS Audit update

Mr Martin Duggan provided a detailed update on the final Scottish Government Network and Information Systems (NIS) Audit which has now been completed. NHS Ayrshire and Arran achieved a final score of 99%, being one of the highest-performing Boards nationally. Auditors commended this result. Key outcomes were as follows:

- Overall compliance increased by 3%.
- All 17 categories and 68 sub-categories achieved compliance levels of 80% or above.
- All categories achieved compliance levels above 90%, with 11 categories reaching 100%.
- A total of 414 controls were achieved, with only two remaining outstanding.

The National Cyber Security Centre's Cyber Assessment Framework (CAF) will replace the current NIS audit approach. Unlike NIS, CAF does not require the same level of evidence, controls, or assessment detail.

Members discussed whether updates on the new framework should continue to be reported to the Committee. It was agreed that reporting would remain in place until the new process is fully established.

Outcome: Committee members noted the summary of the Cyber Security team's activities over the reporting period. Members commended the team for the excellent progress made with the final NIS audit.

6.2 **Information Governance Update report**

Ms Marie Lynch, Head of IG and DPO, provided the Committee members with a combined Information Governance update, and the following areas were highlighted:

Item: Information Security Incident Report

The report covered the period from January to March 2026. During this time 38 information security incidents were reported on Datix, this number is higher than the quarterly average of 25. Key themes were; information being filed incorrectly, being sent to the wrong recipient, or left unsecured. Most incidents were reported within Acute Services and the Partnerships however this is expected given the size of these Directorates and the sensitive nature of the information they process. Ms Lynch advised that the increase during this quarter was not currently a cause for concern, as it may reflect improved reporting. However, incident levels will continue to be monitored.

There were 40 potential inappropriate access incidents identified by the FairWarning system, involving 24 NHS employed staff members. Confirmed statistics were not available by the paper submission deadline.

One data breach was reportable to the Information Commissioner's Office (ICO) during the reporting period. This related to personal information disclosed in an email, which should have been removed before being circulated.

SBAR (Appendix 2)

The SBAR relates to a serious data breach involving inappropriate access to patient records. The inappropriate access was initially identified by the FairWarning system and further investigation found extensive inappropriate access to patient information by a staff member. Records viewed included test results, clinical notes, correspondence and demographic information. Some patients were known to the staff member, while others had no apparent link. The staff member had legitimate system access for their role, but their access to health records exceeded what was necessary for their role. There is no evidence that information was extracted, printed or shared, and the staff member no longer works for NHS Ayrshire & Arran. The breach was reported to the Information Commissioner's Office, Police Scotland and the Scottish Government.

Affected patients were informed by letter and offered telephone support, with around half of those contacting the Information Governance team for further assurance and advice. Several Subject Access Requests were also received. The breach was reported in local media and on social media. The Communications team issued a holding statement for media enquiries.

Following the breach, it was agreed that the previous FairWarning face to face Human Resources meeting process will be reinstated. The Information Governance team is also working with Communications to strengthen staff information and awareness. A Stop Press notice will be issued, and all staff Information Governance training is being progressed.

In response to a question about why the issue had not been identified earlier, Ms Marie Lynch advised that this was due to the records accessed and the way the system is set up. Ms Marie Lynch answered a further question regarding formal complaints and advised that approximately five cases had been handled as such.

Outcome: Committee members noted the breach appeared to have been managed appropriately and related to the actions of an individual staff member, while adding that the organisation should remain mindful of the issues raised.

Item: MAST Safe Information Handling Compliance

Overall compliance has fallen from 78% in February to 59%, reflecting the introduction of the new Once for Scotland module in March and the move from two-yearly to annual revalidation. Compliance is expected to improve month by month, with all staff due to complete the module by March 2027.

Although the previous Information Governance Operational Delivery Group (IGODG) agreed that compliance below the 90% target would be escalated to the Corporate Management Team (CMT), this will not be taken forward at present in light of the recent changes.

In response to a query from a member, Ms Marie Lynch advised that the current compliance position is broadly in line with that of most other Boards. She noted that local compliance had previously been around 78%, but a local target of 90% had been set and continues to be monitored through IGODG.

Item: Record of Processing Activities (ROPA) update
Work to transfer information to the new ROPA template is continuing, with time allocated each week to progress this. However, other operational pressures, including Subject Access Requests, continue to take priority.

The new Information Governance Assurance Officer is now in post to support Corporate Records and Freedom of Information, and the Deputy Data Protection Officer is due to start in June. Subject to a further staff member returning from maternity leave, this will bring the team to full complement.

It remains anticipated that this work will be completed by December 2026, as previously advised.

Item: IG work programme 2026/27 update - Members received an update on the work programme in the following areas:

Public Records (Scotland) Act 2011:

- Element 4 Business Classification Scheme and Element 11 audit trail - are awaiting national SharePoint implementation. There was a timeframe of March 2027, this will not be met and have been advised by the National team that it will be 12-36 months from implementation.
- Element 15 contract clause - a meeting has been arranged with, Digital Services and Procurement to progress this action, and a further update will be provided at the next meeting.

RBACs and Break glass
Review of the Clinical Portal – the papers are complete and due to be discussed at the next Corporate Management Team meeting.

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

Item: Information Commissioner's Office (ICO) audit action plan
The actions have been included in the Information Governance work plan.

7. Corporate Governance

7.1 **Information Governance Committee Annual Report 2025/26**
The Head of IG and DPO, Ms Marie Lynch, presented the Committee's 2025/26 annual report for awareness. The report including a self assessment checklist, assurance mapping report and assurance reporting to NHS Board. The report provided assurance that the

Committee had fulfilled its remit during the year.
This had been another challenging year for the team with continued workforce and workload pressures. The successful recruitment of an IG Assurance Officer, supporting Freedom of Information and Corporate Records Management activity, together with the forthcoming appointment of a Deputy Data Protection Officer, will help the team maintain high compliance across all areas of Information Governance and strengthen relationships across the Board.

The Chair commended the team for delivering their role to a high standard, often under challenging circumstances.

Outcome: Committee members approved the Committee's annual report for onward submission to the NHS Board.

7.2 **Information Governance Operational Delivery Group**
Committee members noted the draft minutes of the meeting held on 02 February 2026. Ms Marie Lynch advised that the draft minutes for the April meeting were not yet available, as the meeting dates had been rearranged. These will be presented at the next Information Governance Committee meeting in August.

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 08 June 2026.

- The action log is up to date and progressing
- Training within cyber security remains low
- NIS audit with a final audit score of 99%
- Supplier vulnerability is a cyber risk, action is being taken
- Data breach by a previous NHS employee

10. Any Other Competent Business

10.1 Dr Crawford McGuffie thanked Ms Eleanor Sands for supporting the Committee and for taking on responsibility for the minutes following changes within the Chief Executive's Office.

Ms Jean Ford suggested that risks reported to RARSAG should be considered at the end of the meeting rather than earlier in the agenda.

Ms Sharon Morrow sought clarification on Linda Semple serving as interim Chair from July to December 2024, and the Committee confirmed that this was correct.

11. Date and Time of Next Meeting

Tuesday 25 August 2026 at 9.30am, MS Teams meeting.

Approved by the Chair, Marc Mazzucco
Date: 25 August 2026