**NHS Ayrshire & Arran**

# Information Governance Committee
**Tuesday 2 May 2023 at 9.30am**
**MS Teams meeting**

| | |
|---|---|
| Present: | Mrs Jean Ford, Non-Executive Board Member (Chair) |
| | Ms Sheila Cowan, Non-Executive Board Member (Vice Chair) |
| | Miss Christie Fisher, Non-Executive Board Member |
| | Mr Marc Mazzucco, Non-Executive Board Member |
| | Cllr Douglas Reid, Non-Executive Board Member – present from item 5.1 |
| | |
| Ex-officio: | Mrs Lesley Bowie, Board Chair |
| | Mr Derek Lindsay, Senior Information Risk Owner |
| | Ms Ann Wilson, Head of Information Governance (IG) and Data Protection Officer (DPO) |
| | |
| In attendance: | Ms Claire Burden, Chief Executive, NHSAA |
| | Mr Derek Gemmell, Assistant Director, Digital Services Item 5.1 |
| | Ms Kate Macdonald, Risk Manager Item 8.1 |
| | Mrs Shona McCulloch, Head of Corporate Governance Item 6.3 |
| | Mrs Angela O'Mahony, Committee Secretary (minutes) |

## 1. Welcome/Apologies for absence

1.1 The Committee Chair, Mrs Jean Ford, welcomed everyone to the meeting, in particular Miss Christie Fisher who had recently joined the Committee. Mrs Ford advised that following changes to Board Members' responsibilities and as she was already Chair of the Board's Audit and Risk Committee, she would be stepping down as Committee Chair but would remain as a Committee member. Mr Marc Mazzucco would be taking over as IGC Chair at the end of this meeting.

1.2 Apologies were noted from Ms Nicola Graham and Dr Crawford McGuffie.

## 2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

## 3. Draft Minutes of the Meeting held on 6 February 2023

The minutes of the meeting held on 6 February 2023 were 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 7.1 (06/02/2023), IT controls internal audit** – Mr Gemmell advised that draft leavers' guidance was in the final stage of preparation before being sent to managers.   Feedback was awaited from National Shared Services about extending the number of Fair Warning licences.  The Committee requested an update at the next meeting **DG**
- **Item 5.2 (06/02/2023), IG work programme** – Ms Wilson clarified in reply to a query that the IG team would have operational responsibility for the IG work programme which would be discussed at the IGODG as required, for example, around procurement opportunities.    Action complete.
- **Item 5.2 (06/02/2023), FOI report** – Action complete.
- **Item 5.2 (06/02/2023), IG update, Record of processing activities (ROPA) –** Ms Wilson clarified that ROPA had already been set up and that this was separate to the Board's work to input information into OneTrust.  It was hoped to have this work completed by the end of May 2023.  Members requested that this action should be divided to reflect progress made and an update provided at the next meeting on progress to transfer information to One Trust.  Ms Wilson will provide a presentation at a future meeting to outline how OneTrust works. **AW**
- **Item 8.1 (29/08/2022), IG Strategic Risk Register** – Ms Wilson updated that following publication of the ICO report, the Board had very specific areas of non-compliance related to IG and an action plan had been developed in response.  The current focus of IG resource would be to prioritise the ICO action plan and areas of non-compliance.   Once the action plan had been completed, the team could re-visit the compliance matrix and areas for improvement.  Action ongoing.

4.2   **IGC Work Plan** – The Committee noted the work plan for 2023-2024.

**5.    Information Governance**

5.1   **Digital/Cyber Security update**

The Assistant Director, Digital Services, Mr Derek Gemmell, presented a summary of the key areas of activity by the IT Security team over the last two months and highlighted the following:
- Patch status on servers and desktop computers remained high and a regime was ongoing.
- Virus detection rates were generally consistent with a number of viruses being picked up by software.  The Board had moved to MS Defender software as virus protection was included with the M365 licence.
- Security Operations Centre alerts – There was a large increase in user behaviour in March 2023 due to a sophisticated single phishing email sent to a number of NHSAA staff.  The website had been blocked and no damage was done.  However, this underlined the need to be alert to phishing emails.  A number of updates had been sent to staff through news alerts and the daily digest.

- Vulnerability scanning – an increased amount of monitoring and management of alerts was being done. Working with CGI the Board had improved NESUS scanning to detect a greater number of vulnerabilities at an earlier stage giving more time for corrective actions to be taken.
- Work was taking place to replace the current Learnpro modules with new Cyber Security awareness training.
- Network and Information Systems (NIS) audit 2023 – the Board required to submit evidence in early February 2024. There would be a physical audit of data control centres. Work was ongoing in response to the recommendations from the last audit.
- The Board's internal auditor was conducting a cyber and security resilience advisory review at present.

Mr Gemmell reassured in response to a question from a member that other than the sophisticated phishing email in March 2023, there were no specific concerns to raise from the cyber security activity summary. In reply to a query, he explained that as other Boards did not publish cyber security data, the Board monitored local trends and took early action to address issues identified. Patch status was high and virus detection was working effectively. The Board's Head of IT Security attended the national Cyber Security group which met regularly to discuss cyber security issues. The Board also worked with the National Cyber Centre and there was rapid exchange of information related to potential cyberattack.

Mr Gemmell clarified in reply to a query from a member that the cyber and security resilience advisory review by internal audit had recently been issued and a management response should be submitted towards the end of May 2023. The Committee would receive an update on progress against the recommendations at a future meeting.

**DG**

An update and progress with the NIS audit actions was requested to be presented at the next meeting.

**DG**

In response to a question from a member, Mr Gemmell explained that as the Board was part of the NHS Scotland national O365 programme, all email was scanned nationally and managed by the national team which was very quick to react and block websites that staff may inadvertently click on through phishing attempts. Locally, education and training was taking place to prevent staff from clicking on links from unexpected emails or users not trusted and to report suspicions to IT security.

> **Outcome:** **Committee members noted the summary of the IT Security team activities over the reporting period. Members looked forward to receiving an update on progress against the recommendations of the cyber and security resilience internal audit at a future meeting.**

5.2 **Information Governance Update report**

The Head of IG and DPO, Ms Ann Wilson, provided the IG update report and highlighted the following areas:

- Record of Processing Activities/Information Asset Register – Work was underway to export the current IAR onto the OneTrust application with the aim to have this populated with ROPAs and IAR entries by mid-May 2023.
- Security Incident report – there had been a slight increase in data breaches which may reflect the work being done to encourage people to report more breaches. The reasons for breaches were similar to previous reports, such as sending information to the wrong person or staff accessing information inappropriately. There were currently no complaints with the Information Commissioner's Office and no notifiable breaches.
- IG Work Programme 2022-2023 – the work programme was led by the IGC team with regular input from other services, such as, Health Records and Procurement. The following updates were provided:

  Public records, it was hoped to progress a service level agreement and memorandum of understanding with Ayrshire Archives and this was still to be ratified.

  Freedom of Information (FOI) – the action related to training had been completed and key performance information for compliance stats for 2023-2024 had been agreed. In terms of benchmarking against other Boards, the latest national data available was for quarter two of 2022-2023. Benchmarking data would be provided in reports going forward.

  A new Sway eNewsletter was launched on 16 February 2023 with practical IG information for staff, including training available. There had been several early expressions of interest for FOI training which was encouraging.

  Ms Wilson highlighted areas of slippage in the work programme related to development of information asset owner training and the OneTrust application, although this was now up and running. She updated that training would be written and delivered to all information asset owners. The new national Data Protection Impact Assessment had been adopted but no national guidance issued. Local guidance would be developed. A DPIA protocol was in draft awaiting ratification. The action related to supporting implementation of O365 was ongoing. This work was co-dependent on national agreements and input as one tenancy.

- Information Commissioner's Office (ICO) audit report and action plan – Ms Wilson gave assurance that good progress was being made and a number of actions had been completed. While there were areas of non-compliance, the Board had already identified these issues through self-assessment and was working through them. The audit had commended NHSAA's approach to security incident breach reporting as an area of

good practice.

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

**Members looked forward to receiving an update on the ICO report and progress against the recommendations as well as areas of risk identified at the next Committee meeting.**      **AW**

## 6. Governance

### 6.1 Information Governance Committee Annual Report 2022-2023

The Head of IG and DPO, Ms Ann Wilson, presented the Committee's annual report for 2022-2023 which set out key achievements through the year in discharging its remit. The report included a self-assessment checklist and, for the first time, the report included assurance mapping and NHS Board reporting to evidence that the Committee had fulfilled its remit.

Committee members received assurance that the Board maintained a high level of compliance in all areas of IG and good progress had been made in maintaining and improving the position during a continued period of system pressures. The Committee had received regular reports to evidence overall levels of compliance and robust processes were in place for monitoring of improvement actions, issues and risk management. No material issues had arisen during the year. A new Head of IG was appointed during the year and had seamlessly settled into her role and continued to drive change and improvement.

Committee members discussed the significantly increased FOI activity compared to last year and variable performance in responding to requests within the target timescale. The Chief Executive updated that as previously agreed with the Committee, she had raised the high number of requests received via MPs' and MSPs' offices with local parliamentarians. She had respectfully reminded them that their offices could obtain information from the Board using information that was already available and did not have to go down the FOI route. Ms Wilson added that the issue had also been discussed at the national FOI forum and the Scottish Information Commissioner's office had agreed to take back through their routes. FOI champion training would be revised and another couple of dates had been advertised through the Sway newsletter for those responding to FOIs, with good uptake so far which was encouraging.

The Committee received assurance that the IG team monitored the number of staff attending FOI training but this was not mandatory. Should any issues be identified, Directors would be asked to nominate staff to join FOI training to raise awareness. The Committee Chair requested that an additional sentence be added to the annual report

related to education and training to ensure this was appropriate to meet business requirements. The Committee would have a role in terms of oversight and awareness should it be identified that additional training was required.

**Outcome:** **The Committee approved the IGC Annual Report 2022-2023 subject to an additional sentence being added related to education and training, to ensure this was appropriate to meet business requirements.**

6.2 **Information Governance Operational Delivery Group**

Committee members noted the draft minutes of the meeting held on 6 February 2023. Ms Wilson highlighted that the group's membership would be widened to include procurement, communications and governance which should enrich the work programme going forward.

6.3 **Document Security Classification Guidance**

The Head of Corporate Governance, Mrs Shona McCulloch, presented draft document security classification guidance for approval. This followed a request from the previous Chief Executive to provide guidance for staff on protective markings, with the aim to ensure a consistent approach and to deliver good governance in protecting the organisation's documents and information they contain.

Mrs McCulloch gave assurance that she had worked closely with the Head of IG in developing the guidance which provided up-to-date advice on document security. The classification system being used aligned with the UK Security Classification Framework although the Board had chosen label names more suited to the Health Care environment. NHSAA also followed the NHS Once for Scotland Green, Amber, Red system for the security classification of documents created within the organisation in keeping with the NHS Scotland email security guidance.

Committee members were advised that the majority of communications would not require labelling, with a minority of documents containing official-sensitive information being protectively marked or document security classified.

The Head of IG, Ms Ann Wilson, explained in reply to a query from a member that the Green, Amber, Red system for email security guidance should be used to alert staff to consider whether information should be marked as official-sensitive.

Members discussed the subjective nature of document classification and it was agreed to monitor the position following rollout of the new guidance. Ms Wilson would discuss with Mrs McCulloch the possibility of carrying out random sampling of documents a couple of times each year to provide a snapshot and to monitor implementation of the new guidance. However, it was recognised that this activity would be resource dependent. Consideration would also be given to rollout of

**AW/SM**

staff training and awareness sessions, including through the IG Sway e-Newsletter.

> **Outcome:** **The Committee approved the guidance and looked forward to receiving an update on plans for staff training and to monitor implementation of the guidance.**

## 7. Audit

7.1 There were no audit reports to discuss.

## 8. Risk

### 8.1 Information Governance Strategic Risk Register

The Risk Manager, Ms Kate MacDonald, presented a report on risk management arrangements and the latest risk register which was discussed and approved at the Risk and Resilience Scrutiny and Assurance Group meeting on 21 April 2023.

Ms MacDonald highlighted that there were two high risks being treated, risk ID 603, service bus interruption - cyber incident which was reviewed in March 2023 and was due for review again in September 2023, and risk ID 557, compliance - Information Governance which was due for review in July 2023. Detailed risk assessments were provided at Appendix 2 of the report. There were no proposed risks for escalation or downgrading and no emerging risks had been identified.

> **Outcome:** **Committee members discussed the report and took assurance from the work being done to manage strategic risks which fall under the Committee's remit.**

8.2 There were no risk issues to report to the Risk and Resilience Scrutiny and Assurance Group.

## 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 23 May 2023:
- IGC annual report
- ICO report
- Suite of routine reports received, including IG update and IGC Strategic Risk Register.

## 10. Any Other Competent Business

10.1 There was no other business. Mrs Ford formally handed over to the new IGC chair, Mr Marc Mazzucco.

## 11. Date and Time of Next Meeting

**Approved by Committee on 18 September 2023**

**Monday 28 August 2023 at 9.30am, MS Teams - changed to
Monday 18 September 2023 at 9.30am, MS Teams**

Signed by the Chair                                              Date:  18 September 2023