Approved by Committee on 29 April 2024

NHS Ayrshire & Arran

Information Governance Committee
Monday 26 February 2024 at 9.30am
MS Teams meeting

Present:	Mr Marc Mazzucco, Non-Executive Board Member (Chair) Mrs Jean Ford, Non-Executive Board Member Mr Ewing Hope, Non-Executive Board Member – attended part of meeting Cllr Douglas Reid, Non-Executive Board Member – attended part of meeting
Ex-officio:	Ms Claire Burden, Chief Executive and Senior Information Risk Owner Ms Nicola Graham, Director of Infrastructure and Support Services Dr Crawford McGuffie, Medical Director, Deputy Chief Executive and Caldicott Guardian
In attendance:	Mr Derek Gemmell, Acting Assistant Director, Digital Services item 6.1 Ms Natali Higgins, Information Governance Manager item 6.2 Ms Marie Lynch, Deputy Data Protection Officer item 6.2 Ms Tara Palmer, Freedom of Information Officer item 6.2 Mrs Angela O'Mahony, Committee Secretary (minutes)

1.   Welcome / Apologies for absence

1.1   The Committee Chair welcomed everyone to the meeting. Mr Ewing Hope, Non-Executive Board Member, joined for part of the meeting to enable the Committee to achieve a quorum.

1.2   Apologies were noted from Mrs Lesley Bowie, Mrs Sheila Cowan, Miss Christie Fisher and Ms Ann Wilson

2.   Declaration of any Conflicts of Interest

2.1   There were no conflicts of interest declared.

3.   Draft Minute of the Meeting held on 13 November 2023

The minute of the meeting held on 13 November 2023 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 action:

Item 5.2, One Trust presentation – As Ms Wilson was unable to join the meeting, this item was deferred to the next Committee meeting on 29 April 2024.

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

5.   Risk

5.1   **Information Governance (IG) Strategic Risk Register**

The Medical Director, Dr Crawford McGuffie, presented the IG Risk Register report.   The report had been discussed in detail at the Risk and Resilience Scrutiny and Assurance Group (RARSAG) meeting on 25 January 2024.

Committee members were advised that there were no changes to the two risks previously allocated to the Committee, with no proposed risks for escalation or downgrading for this meeting.

Dr McGuffie advised that a new strategic risk ID 856 had been approved by RARSAG on 25 January, as detailed at Appendix 2 of the report. This risk related to retention of mailboxes to support the COVID-19 Inquiry. Members received assurance that significant work had taken place to align with the COVID Inquiry's requirements and that mailboxes had been retained for key decision-makers related to COVID who had now left the organisation.   The risk was in the process of being finalised and would be available in the normal format for the next report, including updated assessor date and review date.

Detail around individual risks was provided at Appendix 3 of the report and Appendix 4 provided a severity consequence matrix for members' information.

> **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 RARSAG.

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 up to 31 December 2023 and highlighted the following:

- Work continued to move laptops to Bitlocker encryption and remove McAfee encryption. Defender anti-virus software was being used instead of Sophos, as Defender was included in the M365 package.
- Since the launch of the new Cyber Security Turas module on 1 September 2023, there had been good uptake with 5,051 staff having completed the module which was linked to Learnpro for Mandatory and Statutory Training (MAST) certification. Work would continue to publicise this training.   Mr Gemmell advised in reply to a query from a member that it was expected that all

staff would have completed the module within 12 months and it would have to be repeated every two years.

- The number of devices not logged in for 90 days remained consistent.
- Percentage of patches installed was consistent with previous reports.
- Security Operations Centre alerts showed a small decrease in December. The team continued to monitor and prioritise vulnerabilities which fluctuated on a daily basis.
- A third party product was being used to patch GP services to ensure they remain secure, as they used a number of systems no longer supported by MS, pending the move to the new GP system.
- NHSAA was one of six pilot Boards for Microsoft Security Baseline which aimed to apply a standard of secure controls to Windows devices across the NHS Scotland Tenancy. The pilot was at an early stage and had been applied to a small number of devices on the estate for testing. This should be applied to the full estate from June 2024.
- Network and Information Systems (NIS) Audit 2023-2204 – The Board submitted evidence for the NIS audit on 5 February. The auditor would visit on 13 March to speak to key staff and would report back to the Board on 28 March 2024. The Cyber Security internal audit would be discussed later on the agenda.
- The IT Security team had been rebranded as the Cyber Security team to better reflect the work being undertaken by the team and the modern cyber environment.

> **Outcome:** **Committee members noted the summary of the Cyber Security team's activities over the period up to 31 December 2023.**

6.2   **Information Governance Update report**

Committee members received a combined Information Governance (IG) update and the following areas were highlighted:

6.2.1   **Public Records (Scotland) Act** (PRSA) – The IG Manager, Ms Natali Higgins, provided an update on the Board's compliance with the PRSA 2011. The report set out progress to implement the 15 elements of the Records Management Plan (RMP) to improve the management of the organisation's corporate records. As previously agreed by the Committee, the report covered the following areas that had been highlighted as amber or red (green actions had been completed):

- There were no elements of the plan categorised as red.
- Four areas were categorised as amber, of which element 4 and element 11 were reliant on national implementation of the new M365 platform.
- A national workshop would be held in the near future to discuss rollout of a business classification scheme and this work was likely to take some time before the national rollout could take place.

- Significant national work was required before the new Sharepoint could be implemented.
- There was no progress to report related to element 7, archiving and transfer. Feedback was awaited from South Ayrshire Council related to charges for storage and archiving of material.
- For element 15, third party suppliers, significant work had been done to add new terms and conditions into generic terms and conditions to be adopted by contractors as and when required when producing records on behalf of the Board. Work was planned to identify existing contracts requiring new clauses to be added.

A Directorate improvement plan had been devised with 66 actions split into 10 different requirement areas. This had been developed with input from the CRM Champions Group. The plan had been finalised at the end of August 2023 and was implemented from 1 October 2023. A summary of compliance per Directorate up to 31 December 2023 was provided at Figure 1 in the report.

Ms Higgins highlighted that progress varied significantly across Directorates, with the Medical Directorate, Nurse Directorate, Chief Executive's office and Transformation and Sustainability having made considerable efforts to move forward. Discussion had taken place with other Directorates which were not as far ahead and there were plans in place to progress this work further.

Figure 2 in the report provided an improvement dashboard detailing compliance across the organisation, with some good practice identified as well as areas requiring improvement. Ms Higgins would check information provided related to secure storage areas and update as appropriate. The detailed improvement plan would be included with PRSA updates going forward.

Ms Higgins highlighted that the report provided a Progress Update Review detailing progress to implement the requirements of the RMP which it was planned to submit to the PRSA Assessment Team.

Committee members discussed overall compliance, Directorates making good progress and others where further improvement work was planned. It was hoped to see improved compliance in these areas in future reports. Members discussed storage and underlined the importance of information being organised and searchable.

6.2.2   **Information Security Incident Report**

The Deputy Data Protection Officer, Ms Marie Lynch, provided a report on information security incidents for the period October to December 2023 and highlighted the following areas:

- The quarterly average of security incidents reported for the previous three years was 25, with 35 breaches reported during the reporting period, 23 of which related to personal data breaches. The team would continue to raise awareness of what

- constituted a breach to try to encourage breach reporting.
- The report provided details of breaches across Directorates.
- One breach was considered notifiable to the Information Commissioner's Office which related to a person's information being shared with all patients in a ward due to human error. ICO had reviewed the information and advised that no further action was necessary, although several recommendations had been made related to password protection on multi-use printers, something which the Board already promoted.
- The Board had not yet heard back in relation to a breach that was reported at the last Committee meeting.
- The Information Governance Operational Delivery Group had agreed that a formal action plan would be put in place for ICO recommendations which would provide a record of recommendations made following breaches and actions taken as a result.
- There were no complaints being investigated by the ICO.

6.2.3 **Freedom of Information (FOI) Report** – The FOI Officer, Ms Tara Palmer, provided the routine six monthly FOI activity report and FOI 2023 annual report. The following areas were highlighted:

- There had been a 24% increase in requests compared to 2022, which in turn had seen a 28% increase from the year before, with 1,004 requests in 2023 compared to 811 the previous year.
- The number of requests was consistently increasing year on year, with the same staff resources to manage requests.
- Acute services continued to receive the majority of requests, with around a third of all requests related to Acute.
- Three researchers made up 47% of requests received from MSP offices, which had amounted to 29% of the total requests received last year and currently 22% of requests received.
- Requests continued to be complex and required a response from multiple Directors.
- The report provided a detailed analysis of requests received and compliance in responding to requests within the required timescale.
- Performance in responding to FOI requests had dropped slightly from last year. There were staffing resource issues in the team. However, performance remained good with 93.8% compliance and this level continued to be maintained.
- 92% of queries made received all or some of the information requested, with refusals accounting for 8%. Ms Palmer explained that this could be due to the Board not holding the information or the need to search patient records.
- For the period January to December 2023, NHSAA performance in responding to FOI requests was similar to other similar sized Boards, with all Boards seeing a similar increase in the number of requests received.
- There were six requests for internal review, with one related to a response provided outwith the 20 working days timescale.

Others had related to information withheld for various reasons, such as, commercial sensitivity, all of which had been responded to within 20 working days.

- Members received an update on Office of the Scottish Information Commissioner (OSIC) investigations outstanding from last year. Of the three outstanding investigations, one had been closed. All information had been provided for the other two and it was hoped that these would be completed in the near future. The OSIC was currently experiencing a backlog in appeals, with half of the team working on backlog and the other half on 2024 appeals.

Dr McGuffie advised in reply to a query from a member that the high level of requests received from a small number of Researchers in MSPs' offices had been raised at the last two quarterly meetings with MPs and MSPs. He would consider if targeted discussion should take place with individual MSPs' offices to try to improve the position.

CMcG

The Committee discussed the IG report, specifically progress and areas of challenge related to implementation of the improvement plan. The Medical Director, Dr Crawford McGuffie, reassured members that while there had been delays in taking forward some of this work due to current workload compounded by staff absence, the situation was being actively managed on a risk based approach. This work was set in the context of positive updates around Corporate Records Management, Information Security and Freedom of Information reports.

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

7. Corporate Governance

7.1 Information Governance Committee Terms of Reference (ToR) annual review

The Committee reviewed the Committee's ToR and noted changes made, in particular, to reflect that the Chief Executive, Claire Burden, had taken on the role of Senior Information Risk Owner. The committee was content that the ToR remained appropriate for the current and proposed work over the next year.

Committee members highlighted that discussion was taking place offline about potential areas of crossover between cyber and information security related to the Digital Strategy. This may require to be considered as part of a future review of the Committee's ToRs.

> **Outcome:** **Committee members reviewed and endorsed the changes made to the Committee's ToR for onward submission to the NHS Board for approval.**

7.2 Information Governance Operational Delivery Group

Committee members noted the draft minutes of the group's meeting held on 29 January 2024.

8.   Audit

8.1   Cyber Security and Resilience Internal Audit Report

The Acting Assistant Director of Digital Services, Mr Derek Gemmell, presented the internal audit report completed in 2023 by Grant Thornton on Cyber Security and Resilience.

The audit had examined all aspects of Cyber Security and made a number of recommendations. The auditor had made 10 observations, all of which were already under consideration within the existing NIS audit, with many included in the mitigations related to Information Governance Committee risk ID603, service/business interruption, cyber security. The report provided a detailed update on progress with the 14 advisory actions resulting from the audit. Six of the actions had been completed and four were in progress. Members received a detailed update on work ongoing related to the four advisory actions overdue, with progress being reported regularly through the Strategic Digital Delivery Group.

Committee members discussed the report and it was acknowledged that while some of the work outstanding was being progressed locally, other areas required national work to take place.

Mr Gemmell advised in reply to a query form a member that the Board used a number of clinical systems which were key for clinicians' day-to-day work but which were not compatible with modern operating systems, with mitigations put in place should there be a security risk. The Board was assessing all applications (apps) used with a view to retiring older apps, with clinical involvement in the decision-making process as appropriate.

In response to a question from a member, Mr Gemmell explained that the Board was working towards having a complete list of all software and licences being used in one central database repository.

> **Outcome:**   **Members discussed the internal audit report and noted progress against the recommendations made.**

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 26 March 2024:

- Strategic risk register – addition of new risk ID856
- Information Governance Committee Terms of Reference – supported change to reflect that the Chief Executive, Claire Burden, has taken on role of Senior Information Risk Owner.
- Information Governance update - Information Commissioner's Office action plan –progress with the plan. Delays in taking

forward some work due to current workload compounded by staff absence. Situation being actively managed on a risk based approach. This work is set in the context of positive updates around Corporate Records Management, Information Security, and Freedom of information Reports.

10.   Any Other Competent Business

10.1   There was no other business.

11.   Date and Time of Next Meeting
Monday 29 April 2024 at 9.30am, Room 1, Eglinton House, Ailsa Hospital, Ayr

Signed by the Chair: Date: 29 April 2024