

Information Governance Committee
Monday 18 September 2023 at 9.30am
MS Teams meeting

Present: Mr Marc Mazzucco, Non-Executive Board Member (Chair)
Miss Christie Fisher, Non-Executive Board Member
Mrs Jean Ford, Non-Executive Board Member

Ex-officio: Mrs Lesley Bowie, Board Chair
Ms Claire Burden, Chief Executive and Senior Information Risk Owner
Ms Nicola Graham, Director of Infrastructure and Support Services
Dr Crawford McGuffie, Deputy Chief Executive, Medical Director and Caldicott Guardian
Ms Marie Lynch, Deputy Data Protection Officer (DPO), Information Governance

In attendance: Mr Derek Gemmell, Assistant Director, Digital Services
Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Welcome / Apologies for absence

1.1 The Committee Chair welcomed everyone to the meeting.

1.2 Apologies were noted from Mrs Sheila Cowan, Cllr Douglas Reid 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 2 May 2023

3.1 The minute of the meeting held on 2 May 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.

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

5. Risk

5.1 Information Governance Strategic Risk Register

The Deputy Chief Executive and Medical Director, Dr Crawford McGuffie, presented the latest version of the Strategic Risk Register for Information Governance (IG) risks. The Risk and Resilience Scrutiny and Assurance Group (RARSAG) had conducted an in-depth

review of all organisational strategic risks at its meeting on 21 July 2023. It had been agreed that the two high level IG risks being treated should remain on the Strategic Risk Register.

Dr McGuffie gave assurance of the Board's commitment to continue to improve the risk management process, and to consolidate assurance, scrutiny and challenge of strategic risk in line with the national Blueprint for Good Governance.

Committee members discussed the IG risk register in detail, particularly in relation to consequence and likelihood and the impact of control measures on the risk rating. The Director of ISS, Ms Nicola Graham, gave assurance in reply to a query from a member that a range of control measures were in place to constantly manage ongoing cyber security threats and to maintain the risk level.

Dr McGuffie explained that the risk register report was a dynamic, live and constantly evolving document. He reassured members that work was planned to update the final assurance statement on the control framework, mitigations in place and their effectiveness. He would feed back the Committee's comments on consequence and likelihood to the Risk Management team for consideration in future review of IG risk. Members requested that the detailed risk matrix be provided in future IG risk register reports.

Outcome: Committee members discussed the report and were assured of the work being done to manage strategic risks which fall under the IGC's governance remit.

5.2 **Risk issues to report to the Risk and Resilience Scrutiny and Assurance Group (RARSG)** - 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 a summary of key areas of activity undertaken by the IT Security Team over the last two months and highlighted the following areas:

- Good progress being made in the replacement of laptop encryption software to Bitlocker.
- New MS Defender anti-virus software has now been installed on the vast majority of devices.
- IT security Learnpro module – this would move to a Turas-based model from 1 October 2023. All staff would require to complete the new module every two years going forward. The changes would be communicated through the Daily Digest and other internal communication, as well as through the Digital Champions network.
- A detailed update was provided on Security Operations Centre (SOC) alerts.

In reply to a question from a member about devices not being logged on in 90 days, Mr Gemmell reassured that staff are regularly reminded to log on to their device. While the number of devices not logged on was at a constant level, this involved different devices. Staff are encouraged to bring their device in to the workplace every 30 days for updates. Should staff not log on for a significant period of time, the device could be deactivated or their line manager could be contacted with a request to return the device. Ms Graham added that this could be an issue for staff working remotely but not logging on to the network via their VPN. Tools are being deployed via M365 to pick up these devices when not logged on through VPN.

Committee members discussed and acknowledged the significant audit work taking place within Digital Services related to Cyber Security.

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

6.2 Information Governance Update report

The Deputy Data Protection officer, Information Governance, Ms Marie Lynch, presented the combined update report and highlighted the following areas:

6.2.1 Corporate Records Management update

Due to other competing priorities and limited staff resource, the Progress Update Review (PUR) was not submitted in February 2023 as planned. The PUR mechanism provided a structured system to manage informal review of agreed Record Management Plans (RMP) and support compliance with Element 13, assessment and review, but it was not compulsory. There were plans to submit the PUR in January 2024. Committee members requested that the Committee should be advised if it would not be possible to meet this timescale.

The report detailed progress with the RAG status of RMP elements. There were no red elements and four amber elements. These related to the business classification scheme; archiving and transferring; audit trail; and public records created or held by third parties, with progress updates provided in the report. All other elements were green.

Ms Lynch highlighted the positive work taking place in NHSAA related to corporate minute taking, with a minute takers network established to develop minute taking guidance and training for staff. This followed a Board level review of minutes in preparation for the COVID-19 Inquiry which had identified the need to improve quality and consistency of minutes.

A dynamic action plan had been developed to support RM Champions to implement, monitor and capture RM improvement in their respective Directorates. This would enable benchmarking to take place to identify areas of good practice as well as areas for improvement and ensure a consistent approach across the organisation.

6.2.2 Information Security Incident Report

The report covered the period April to June 2023. There were 25 information security breaches during this period, with 24 classed as personal data breaches. The trend was similar to quarterly data over the last three years. As previously reported to the Committee, the number of breaches appeared low relative to the size of the organisation and the team had used various methods to raise awareness and encourage breach reporting. Following a slight rise in the last quarter, this had not continued as a trend and further awareness raising would take place.

There were no breaches considered to be notifiable to the Information Commissioner's Office (ICO). NHSAA had no complaints being investigated by the ICO.

6.2.3 Freedom of Information (FOI) report

Committee members received the six monthly update on FOI activity and the FOI annual report for 2022-2023. The Board continued to see a significant rise in FOI requests and this has had a minor impact on compliance in the timescale for responding to requests, currently sitting at 91%. FOI activity was supported by the wider IG team and the increasing number of requests negatively impacted on the team's ability to provide support to departments and input to national work programmes due to the limited resource available. Additional staff resource has been requested, with part of the required recurring budget identified from the current IG staff budget.

There were five requests for internal review in the first half of 2023, including submission for review for requests received in 2022. One was due to the Board not responding within the statutory 20 working days timescale and the other four related to information being withheld for various reasons, as detailed in the report. All internal reviews were responded to within the statutory 20 working days.

Committee members discussed the significant number of FOI requests from MSPs' offices. The Deputy Chief Executive and Medical Director, Dr Crawford McGuffie, advised that this had been raised at one of the quarterly meetings with MSPs and MPs to highlight that some of the information being requested is already readily available and it would be raised again at the next meeting.

Dr McGuffie advised that Natali Higgins, Information Governance Manager for Corporate Records, had recently received the UK Information and Records Management Society's Professional of the Year Award and he commended her for this significant accolade.

Committee members discussed the FOI process and challenges in receiving information from services to enable responses to be sent in a timely manner. Members suggested that the team could link with the Patient Experience team to discuss improvement work being done by their team and any shared learning opportunities.

6.2.4 **Update on Information Commissioner's Office (ICO) action plan -**

The Committee received an update on the Information Commissioner's Office audit report and action plan. Members received assurance that in spite of the capacity and workforce pressures facing the team which had resulted in some actions being paused, overall positive progress was being made in taking forward the action plan. The Board was making similar progress compared to other Board areas.

Members received a detailed update on actions in progress related to A04, review of policies and procedures, A06, to ensure that all processors comply with the terms of written contracts and A09, to review the layout of data sharing agreements. Some of these actions would involve significant work and discussion was ongoing about how to manage this.

In reply to a query from a member, the Deputy Chief Executive and Medical Director, Dr Crawford McGuffie, advised that he would seek an update from colleagues in regard to action A04, and the timescale for approval of the Board's document control policy, to enable this action to be closed off. This would allow the team to focus on priorities involving larger pieces of work.

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

7. **Governance**

7.1 **Information Governance Operational Delivery Group (IGODG)**

Committee members noted the approved minutes of the IGODG meeting held on 21 April 2023 and the draft minutes of the meeting held on 24 July 2023.

8. **Audit**

8.1 There were no audit reports to discuss.

9. **Key items to report to NHS Board**

9.1 Committee members agreed that the following key items be reported to the NHS Board meeting on 9 October 2023:

- IG risk register - work planned to update the final assurance statement on the control framework.
- Update on progress with ICO action plan.
- To highlight the range of Cyber Security audit work taking place.

10. **Any Other Competent Business**

10.1 There was no other business.

11. **Date and Time of Next Meeting**
Monday 13 November 2023 at 9.30am, MS Teams

A handwritten signature in black ink, appearing to be 'M. J.', written over a light-colored rectangular background.

Signed by the Chair

Date: 13 November 2023