Approved by Committee on 6 February 2023

Information Governance Committee
Monday 14 November 2022 at 9.30am
MS Teams meeting

Present: Mrs Jean Ford, Non-Executive Board Member (Chair)
Ms Sheila Cowan, Non-Executive Board Member (Vice Chair)
Mr Marc Mazzucco, Non-Executive Board Member
Cllr Douglas Reid, Non-Executive Board Member

Ex-officio: Mr Derek Lindsay, Director of Finance and 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 Robert Bryden, Health Records Manager
Mr Hugh Currie, Assistant Director, Occupational Health, Safety and Risk Management
Mr Derek Gemmell, Acting Assistant Director, Digital Services
Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Apologies for absence

1.1 Apologies were noted from Mrs Lesley Bowie, 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 Minute of the Meeting held on 29 August 2022

3.1 The minutes of the meeting held on 29 August 2022 were approved as an accurate record of the discussion.

4. Matters Arising

4.1 **Information Governance Committee (IGC) Action Log 2022** - The action log had previously been circulated to members and all progress against actions was noted. Committee members received an update on the following actions:

Item 8.1 (29/08/22), IG Strategic Risk Register, Accountability Framework – Mrs Wilson advised that following the change of Information Commissioner, a different approach was being taken and a new online scoring tool was currently being worked through. A new checklist had been developed and this will be provided at the meeting on 6 February 2023.

Item 8.1 (29/08/22), Strategic Risk Register, Cyber Security risk rating – Mr Gemmell advised that the risk rating would remain unchanged and this reflected the prevention steps and investment in products to improve cyber security in recent years. The risk will be reviewed in March 2023. Action complete.

Item 5.1 (29/08/22), Digital/Cyber Security – The NIS auditor had advised that while some actions could be green, overall there were still elements that required to be progressed before the action was fully achieved. Mr Gemmell advised that the governance and reporting route for the NIS audit recommendations will be through the Digital Programme Management Group and Integrated Governance Committee.

The Chief Executive clarified in response to a question from a Committee member that the Information Governance Committee was responsible for the oversight of information governance elements of Cyber Security to ensure the organisation and sub-contractors are complying with data protection regulations in handling patient and private information. Digital transformation work will be reported through the Integrated Governance Committee. The Committee's Terms of Reference will be updated to clarify its responsibilities related to Cyber Security.

4.2 **IGC Work Plan 2022-2023** – Committee members noted the work plan. It was noted that some IG reports had been amalgamated to rationalise the number of reports being presented while continuing to provide the Committee with the appropriate level of assurance. The Committee supported the new reporting format.

4.3 **IGC Meeting Dates 2023-2024** – Committee members approved the meeting dates.

5. Information Governance

5.1 Digital/Cyber Security update

The Acting Assistant Director, Digital Services, Mr Derek Gemmell, provided a summary of the key areas of activity undertaken by the IT Security Team over the last three months.

Mr Gemmell reported that the number of viruses being detected remained high which underlined the need to continue to monitor and manage alerts. Significant effort had been made to improve patch status of servers and PCs and the position had improved considerably since April 2021.

The report highlighted alerts identified by the Security Operations Centre in October 2022. Following investigation, there was one malicious alert related to a user clicking a malicious link in a phishing email. The link was blocked and an endpoint scan run. There was nothing malicious found on the pc and no further action was required.

The Committee was advised that approval was being sought through the Corporate Management Team (CMT) to replace the current Learnpro IT security module with a tailored National Cyber Security Centre Cyber Security module which could be accessed via Turas. It was proposed that staff training should move from a once only option to every two years. Once CMT has approved the change, it should take place from early 2023.

Engagement had been undertaken with a private supplier to provide Cyber Security Exercise in a Box sessions specifically targeted at Board Members, with dates to be confirmed early next year.

Mr Gemmell advised that work was underway to deploy Active Directory Password Management, a tool to encourage staff to use secure passwords when they are re-setting these in the future.

A job evaluation and recruitment process has been ongoing for a new Senior Technical Specialist – IT Security since the previous incumbent left the organisation in May 2022. Although a current member of the team was acting up in role, this left the team a senior member of staff down.

Committee members discussed the report and welcomed the additional detail provided on the control measures in place to monitor and manage viruses and vulnerabilities.

Mr Gemmell advised in response to a question from a Committee member that there had been a global increase in the vulnerabilities of different products, including MS Office, and while software suppliers were trying to strengthen their products against vulnerabilities, this increasing trend was likely to continue.

The Director of Finance and SIRO, Mr Derek Lindsay, highlighted that Counter Fraud Services had previously run webinars on site related to cyber security and he would ask if it would be possible to run these again. **DL**

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

5.2 **Health Records update**

The Health Records Manager, Mr Robert Bryden, provided an update on Health Records Services activities that fall within the remit of the Board's IG function. The report had not changed since the update provided at the last IGC meeting.

Mr Bryden advised that he had discussed future reporting arrangements with the Committee Chair. It was noted that these reports focused on operational matters which were previously presented to the Information Governance Operational Delivery Group (IGODG) before it was stood down at the end of 2018. It was proposed that now that the group has been re-established, future reporting should resume through the IGODG, with exception reports to the Committee as required. Committee members will be able to continue to monitor progress against this and other areas of operational work through the IGODG minutes provided to the Committee.

Outcome: **Committee members noted the update and approved the proposal that future reports on Health Records Services activities that fall within the remit of the Board's IG function should be presented to the IGODG, with exception reporting to the Committee as required.**

5.3 **Information Governance (IG) Update**

The Head of IG and DPO, Ms Ann Wilson, provided an assurance report in respect of the Board's IG obligations. The report had been re-designed to combine all IG reporting within one report. Committee members supported the change to the format of future IG reports.

Ms Wilson highlighted that the Information Commissioner's Office (ICO) would visit NHSAA in February 2023 to audit the Board's compliance with DP obligations. This would include face to face interviews with relevant staff. Preparatory meetings would take place with staff before the visit, as well as staff debriefing once the audit had taken place. Prior to the audit, the Board would provide evidence to demonstrate accountability and compliance by 23 January 2023 and work is ongoing to meet this deadline.

Ms Wilson explained in response to a question from a Committee member that the audit may highlight gaps in the Board's compliance, for example, DP issues related to legacy contracts with third party suppliers which pre-date General Data Protection Regulations. ICO expertise and feedback would support the Board to address control areas requiring action to mitigate information risks and improve compliance.

The report outlined activity related to completion of Information Asset Registers (IAR). Ms Wilson advised that this work had lost traction due to lack of functionality and other technical issues with the Adobe platform used to host IAR, and it had been agreed that a new platform had to be sourced. A project was ongoing within NHSAA to use OneTrust, for which National Shared Services paid the licence, and all NHS Boards could use to provide a register of processing activities (ROPA). Ms Wilson advised in response to a question from a Committee member that while the lack of traction on IAR was an area of risk for the Board. Creating a ROPA would ensure compliance and support the ongoing development of an IAR for the Board.
Committee members received the security incident report for Quarter 2. There were 28 information security breaches during the reporting period, with one considered notifiable to the ICO. This was due to human error by the processor which led to a technical error. Work is

taking place to mitigate the impact and ensure no harm comes to patients. The breach had also been reported to the Scottish Government. There were no complaints being investigated by the ICO.

Ms Wilson advised in response to a question from a Committee member that she would check whether the information security breaches within East Ayrshire Health and Social Care Partnership related to Caldicott confidentiality and data protection related to Primary Care and provide an update to members out-with the meeting. **AW**

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

6. Governance

6.1 **Information Governance Operational Delivery Group**

As the meeting scheduled for 28 October 2022 was cancelled due to the funeral of HM The Queen, there were no minutes available.

7. Audit

7.1 There were no audits to report to discuss.

8. Risk

8.1 **Information Governance Committee Strategic Risk Register**

The Assistant Director, Occupational Health, Safety and Risk Management, Mr Hugh Currie, presented a report on risk management arrangements and the updated IGC risk register. The report was discussed and approved at the Risk and Resilience Scrutiny and Assurance Group on 21 October 2022.

Mr Currie advised that there were two high IG risks being treated. Risk ID 557, Compliance-Information Governance, was not reviewed during this reporting period and is due for review in January 2023. Risk ID 603, Service/Business Interruption-Cyber Incident, had been reviewed and the only change made was to the Risk Manager.
Mr Currie reassured that this risk was being well managed and reviewed regularly, and a number of control measures were in place to mitigate the risk. The next review date will be in March 2023.

The Acting Assistant Director, Digital Services, Mr Derek Gemmell, will update the Lead Director assurance statement as part of the next review to give additional assurance to the Committee in relation to the effectiveness of the control measures in place to mitigate the risk. **DG**

Outcome: **Committee members discussed the report and took assurance from the work being done to manage strategic risks which fall under the governance remit of the Information Governance Committee.**

8.2 **Risk issues to report to Risk and Resilience Scrutiny and Assurance Group**

There were no risks 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 28 November 2022:

- Cyber Security update, including details of control measures in place to monitor and manage viruses and vulnerabilities.
- Health Records report – agreed future reporting to be through IGODG.
- Regular reports on ICO audit; IAR update and Security Incident report, as well as IG Risk Register report. No major concerns arising from reports.

10. Any Other Competent Business

10.1 There was no other business.

11. Date and Time of Next Meeting

Monday 6 February 2023 at 9.30am, MS Teams

Jean m ford

Signed (Chair) Date: 6 February 2023