BOARD OF DIRECTORS - PUBLIC

SUMMARY REPORT	Meeting Date:	24 July 2024
	Agenda Item:	22

Report Title:	**Digital Assurance Group Annual Report (Incorporating SIRO and Caldicott Annual Reports) 2023/24**	
Author(s):	Phillip Easthope, Executive Director of Finance	
Accountable Director:	Executive Director of Finance (SIRO)	
Other meetings this paper has been presented to or previously agreed at:	**Committee/Tier 2 Group/Tier 3 Group**	Audit and Risk Committee (ARC) Digital Assurance Group
	Date:	16th January 2024 18th December 2023
Key points/ recommendations from those meetings	A significant proportion of this report is taken from the Digital Assurance Group: Review of effectiveness 2023/24. To provide a summary view of our overall cyber security position. Audit & Risk Committee were assured by the report which fed into the Audit and Assurance Committee Annual Report May 2024. The committee noted: Positive Assurance on the progress made with Subject Access Requests (SARS) and Freedom of Information Requests Risk. Following receipt of the Annual Report ARC received assurance that the backlogs had been cleared in the Committees May AAA (Alert, Advise, Assure) assurance report from DAG. Areas for Improvement included the above risk and Data, Security Protection Toolkit outcome to be overseen by the Digital Assurance Group (DAG) Following a year of operation of the new Digital Assurance Group the review indicated the information governance and cyber security governance needs strengthening and a specific group will be reformed. This will go through appropriate governance in early 2024/25. The DAG will report to the Finance and Performance Committee (for overall digital strategy and technical infrastructure) and the new group with report to ARC (for matters of Information Governance and Cyber Security)	

Summary of key points in report

This annual report from the Digital Assurance Group (DAG) incorporates assurance from the Senior Information Risk Owner (SIRO) to the Trust in relation to the effectiveness of controls for Information Governance (IG), data protection and confidentiality. The SIRO has executive responsibility for information risk and information assets and is supported in this work by DAG.
In addition, this report provides an overview of the range of requests directed to and advice sought from our Caldicott Guardian.

The format of this report aligns with the annual work plan used by DAG to form its agenda and reporting schedule. The report highlights work that has taken place over the last year and considers key areas for improvement or discussion over the next year.

This report covers the self-effectiveness review from the Digital Assurance Group (DAG) for 2023/24 and provides:
Key reports, decisions, action plans and third-party reports

- a chronology of key decisions/actions taken in meetings is presented in section 2.1 - the DAG handled a large quantity of work to fulfil its objectives throughout the year.
- section 2.2 presents third-party reports received by the DAG.

DAG would like to emphasise that only one data and information incident warranted reporting to the Information Commissioner's Office (ICO) within the period. The incident was reviewed and the ICO decided that no further action was necessary. This information is offered as positive assurance.

DAG has overseen the improvements made in areas it targeted in 2023/24:
DSPT training compliance delivered the 95% target for the 1st time,
Reduced and subsequently eliminating in May 2024 the backlog in relation Freedom of Information (FOI) & Subject Access Requests (SARs),
Delivered against the Data Security Protection Toolkit action plan except for areas impacted by the delays to implementing the new Electronic Patient Record.

Recommendation for the Board/Committee to consider:

Consider for Action		**Approval**		**Assurance**	**x**	**Information**	

To note assurance on our overall cyber security position. Assurance against Information Governance requirements placed on the Trust, particularly by the National Data Guardian (NDG) standards.
Our current self-assessment shows moderate assurance as part of the DSPT internal audit, substantial assurance on 8/10 standards. Challenges around managing data access and IT protection will be mitigated by the Electronic Patient Record replacement and relate to the Board Assurance Framework risk 0021b.

Please identify which strategic priorities will be impacted by this report:

Effective use of Resources	*Yes*	***X***	*No*	
Deliver Outstanding Care	*Yes*	***X***	*No*	
Great place to work	*Yes*	***X***	*No*	
Ensuring our services are inclusive	*Yes*	***X***	*No*	

Is this report relevant to compliance with any key standards? | **State specific standard**

Care Quality Commission Fundamental Standards	*Yes*	***X***	*No*		Review contributes to understanding of our position under well led
Data Security and Protection Toolkit	*Yes*	***X***	*No*		DAG was the governance group with oversight for our adherence to national data guardian standards and the DSPT

Any other specific standard?	*Yes*		*No*	*X*	

Have these areas been considered? YES/NO					If Yes, what are the implications or the impact? If no, please explain why
Service User and Carer Safety, Engagement and Experience	*Yes*	*X*	*No*		Effectiveness of the DAG had a direct impact on how we protect service user data and the availability of our systems which are a critical part of providing care
Financial (revenue &capital)	*Yes*	*X*	*No*		Report relates to review of meeting effectiveness
Organisational Development /Workforce	*Yes*	*X*	*No*		Report relates to review of meeting effectiveness
Equality, Diversity & Inclusion	*Yes*	*X*	*No*		Report relates to review of meeting effectiveness
Legal	*Yes*	*X*	*No*		Effectiveness of the DAG, through its decision-making and monitoring, provides assurance of our compliance with statutory requirements
Environmental Sustainability	*Yes*	*X*	*No*		Report relates to review of meeting effectiveness

Data & Information Governance Annual Report (including SIRO and Caldicott Annual Reports) 2023/24

Introduction
The structure of the report follows the annual workplan of the Digital Assurance Group (DAG).

DAG is accountable to:
• ARC for matters related to information governance and cyber security.
• Finance & Performance Committee for matters related to digital strategy and technical infrastructure.

The workplan ensures that all the relevant areas of data protection, security and information governance are monitored by the group and appropriate programmes of work or individual actions are agreed as required.

Embedding Information Management and Information Governance
In line with the UK General Data Protection Regulation (GDPR) and the National Data Guardian's data security standards incorporated into the Data Security and Protection Toolkit (DSPT), the Trust maintains formalised processes for managing and sharing data. This includes the adoption of standard operating procedures for the implementation of Data Protection Impact Assessments (DPIA), Data Processing Agreements (DPA) and Information Sharing Agreements (ISA).

Information Governance (IG) Dashboard
Dashboard provides assurance on Information Governance training compliance, server patching compliance, Windows updates, any Phishing incidents, ongoing reporting of Insight document loss / deletions log and monitoring of DSPT audit actions. The Dashboard is reviewed at the DAG meetings and matters reported to ARC through the AAA assurance report.

Standard Operating Procedures
Standard procedures are in place for DPIAs, ISAs and DPAs. The Data Protection by Design (DPD) log captures all the activity taking place as part of these processes as well as decisions made by our Caldicott Guardian. The aim of the DPD log is to provide regular assurance to DAG and evidence for the DSPT assessment.

Data and Information Risks and Incidents
The Board Assurance Framework (BAF) risk and corporate risk register risks along with other directorate level information risks are presented to each meeting of DAG with escalations to the corporate risk register and ARC as required. Improvements to the reporting of risk have been made to include a 'risk analysis' section, which considers the actions required or barriers to achieving the target score.

Section 2: Key reports, decisions, action plans and third-party reports

Key reports received in the financial year and decisions taken

2.1 DAG has a standing agenda and receives the following routine reports on a monthly basis:-

Chief Digital Information Officer's Overview: for assurance. Report acts as an introductory position statement on the current priorities of the Digital department and presents operational information relating to resource availability, capacity and/or capability (i.e. departmental sickness absence data, mandatory training compliance, supervision compliance, recruitment and vacancies).
Digital risks with a current risk score of 9 or above are presented in the report for oversight and to provide DAG with an opportunity to confirm or challenge.

• **Digital Projects Highlight Report**: for assurance and to seek input. It serves as a mechanism for tracking and summarising the progress and status of various Digital projects within the organisation. It provides a concise overview of ongoing initiatives, including the RiO project, highlighting key milestones, challenges, and resource allocations. By offering this comprehensive view, the report enables the committee to assess the financial and operational implications of these Digital projects, ensuring informed decision-making and alignment with the organisation's strategic goals.
Decisions taken in meetings to date:
DAG agreed that time spent on data migration by Data & Warehouse Reporting Project staff should be allocated to New EPR budget (Aug 2023 meeting)
DAG approved a revised completion date, 01/10/2023, for the remaining sites under the Wi-Fi Refresh project (Aug 2023)
DAG approved a delivery date of 30/10/2023 for the Escrow project (Aug 2023). This was later postponed due to budgetary implications.
DAG agreed that the go-live for the SAR module on Infreemation should be split into 2 tranches (Aug 2023)
DAG supported the establishment of a small project board to oversee the update of the mobile device usage policy – Oct 2023.

• **Information Governance Report:** for assurance and to seek input. It provides an overview of performance, assurance and matters of concern re. Information Governance (IG), including updates on Information Sharing Agreements, Data Protection Impact Assessments, the Data Security Protection Toolkit, Freedom of Information and Subject Access Requests (including recovery plan progress), IG policies and IG Incidents.
Decisions taken:
DAG supported inclusion of a dedicated FOI section within the Records Management Policy (Jul 2023)
DAG supported the recommendation to stand down the Data & Information Systems Asset Management Policy in favour of a Standard Operating Procedure (Jul 2023)
DAG approved the IG Audit schedule 2023/24 (Aug 2023)
DAG supported the recommendation that one appropriate health professional conducts the clinical review of records for a SAR process that complies with the law (Aug 2023)
DAG supported the revised Records Management Policy for onward submission to the Policy Governance Group, subject to agreement from the Senior Information Risk Owner (Sep 2023)
DAG supported the recommended list of key performance indicators for regular compliance reporting of FOI and SARs (Sep 2023)
DAG supported the extension of review dates to 29/02/2024 for both the Data and Information Quality Management Policy and the Data and Information Sharing, including Email, Policy (Oct 2023)

We have published our DSPT submission for 2022/23.

There are 4 mandatory requirements which we haven't met, as follows:

DSPT Reference	Requirement
4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.
7.2.1	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.
8.1.3	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted, regularly reviewed and signed off by the SIRO.
9.3.1	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.

An improvement plan is in place and we are therefore “Approaching standards”. The action plan is monitored through the internal audit action process at the time of the annual report action relating to 4.5.4 remains outstanding and will be resolved when our legacy clinical system is replaced.

The Data Security & Protection Toolkit requires the Trust to produce a Training Needs Analysis (TNA) to demonstrate that IG training and awareness activities form part of our mandatory training requirements.

Historically, achieving the mandated 95% training compliance has been very difficult not only at SHSC but across the NHS. 2023/24 was the first year in which 95% compliance was achieved.

• **Information Governance Dashboard:** IG Reporting and Dashboard covers reports compliance to DAG regarding, national CareCert alerts, Phishing Incidents, Windows Infrastructure Patching levels, Windowss Operating system updates; Incidents e.g. infrastructure outages and progress on technical changes.

Compliance in these areas has been good, the notable issue remains as the 2012 servers supporting the clinical system Insight which will be decommissioned following implementation of the new Electronic Patient Records (BAF risk 021a)

• **IT Infrastructure & Operations Report**: for assurance and to seek input. It serves as a comprehensive overview of the organisation's IT landscape and encompasses monitoring of IT infrastructure, security measures, and patching and maintenance activities, providing insights into system performance and uptime. Additionally, the report addresses incident response procedures and outlines future plans for IT initiatives.
Decisions taken:
DAG supported the rollout plan for the Windows 10 feature upgrade to 22H2 (Sep 2023).

• **Service Desk Statistical Report**: for assurance. Reports monthly activity for all Incidents and Service Requests logged by the Service Desk via the SunRise IT Service Management application.
• **New EPR (RiO) Update**: for assurance. The EPR Programme Board report provides updates and insights into the implementation and performance of RiO within the organisation. It offers a comprehensive overview of the project's status, resource allocation, and any challenges or delays encountered. This report is essential for keeping stakeholders, including the Finance and Performance Committee, informed about the progress of the EPR system, allowing them to assess its financial and operational implications, make informed decisions, and ensure that the system aligns with the organisation's strategic objectives and patient care goals. The New EPR Programme reports directly to the EPR Programme Board. DAG receives the report for assurance. This will be the case until the programme has been delivered.
Ad hoc reports received by DAG:
• **Discharge Medicines Service (DMS)**, Aug 2023: DAG members received the paper, supported by the Chief Pharmacist, and approved a decision to start up a DMS project. DAG agreed the project should be stood up in Quarter 4 2023/24 and completed by end of Q4.
• **Alcohol Screening Tool proposal** (Sep 2023): options paper for decision. DAG was asked to assess whether SHSC can continue to maintain the tool (clinically and managerially) in light of the transfer of substance misuse services out of SHSC. DAG supported option 4 as the preferred direction of travel – to continue to maintain the existing tool until the move to RiO, when AUDIT can be built within it for use of SHSC staff only.
• **HR Personal Files: management system proposal:** presented to DAG to seek input and support in vetting a supplier and ensuring a system is fit for purpose prior to the proposal being taken to the Business Planning Group. IT, IG and Procurement colleagues within DAG proffered support outside of the meeting.
• **Dataset Returns: centralised approach proposal**: presented for decision – to agree a standardised approach for the production of clinical dataset returns resulting in improved data quality and greater assurance around the accurate and timely submission of such returns. DAG supported the approach but agreed that it was a matter for decision by the Digital department itself.

Action plans and third-party reports received in the financial year:

2.2 Third-party reports received by DAG 2023/24

• Healthcare Information & Management Systems Society – Analytics Maturity Adoption Model (HIMSS - AMAM), Jul 2023: assessment conducted and presented by Ideal. SHSC achieved a level 0 score (Scores are rated 0 low-7 high) in any of the stages that were assessed (data content, infrastructure, data governance and analytics competency). It was recommended that SHSC undertake a HIMSS INFRAM (Infrastructure Adoption Model) digital maturity assessment prior to implementing the New EPR, followed by a HIMSS EMRAM (Electronic Medical Record Adoption Model) digital maturity assessment before revisiting the HIMSS AMAM.
• **Penetration Test Remediation Plan, Jul 2023**: presented for assurance and visibility of the vulnerabilities identified by the annual security penetration testing audit. The West Midlands Ambulance Service was commissioned to conduct the test. An overall assurance opinion of 'Requires Improvement' was given. The report stated that the 'the opinions provided within this report are broadly similar to those provided to comparable organisation types and environments'.

Section 3: Areas of improvement

3.1 Review of effectiveness. Responses and comments from the self-assessment questionnaires completed by DAG members / regular attendees:
There was a low response rate but emerging themes point to the following areas for improvement:-
• Function / purpose of the group – there is some confusion as to whether DAG is an assurance group or a decision-making body. The Terms of Reference will be reviewed and a Work Plan will be formed for 2024/25.
• Membership of the group – DAG will consider whether its wider audience of regular attendees exacerbates discussions.
• Volume of business – the agenda is vast, a Work Plan will help to manage time and underscore the purpose of papers which in turn will make reporting more effective.
• Relationship to ARC – there is no Executive attendance at DAG (in contrast to the former DIGG and DSG where both the SIRO and Caldicott Guardian attended). As a result, there is an absence of two-way engagement between DAG and ARC and the group does not receive feedback on the reports it sends to the committee.

Section 4: Current risks

4.1 The following matters have been reported to ARC via the Alert, Advise, Assure report submitted to the January meeting and are reiterated here:-
• There is significant risk related to the RiO project which has experienced delays, incurred budget overruns and faces resource constraints.
• There is concern regarding the backlog of Freedom of Information (FOI) and Subject Access Requests (SARs), which, despite recent progress remains at risk.

Section 5 Overall Cyber Security position

DSPT is a good guide to our overall cyber security position and we continue to demonstrate that we have a good understanding of our risks, are transparent about our position and do not have any known critical risks outside of our in-house Electronic Patient Record (EPR). And acknowledging the replacement of the EPR is the priority and will significantly mitigate the BAF and some corporate risks including the key issues identified in the DSPT, the question of whether we are simply mitigating or managing our risks or have a proactive and strategic approach to information security and is one where we must step outside of the limited view that DSPT provides.
Every new service is likely to involve some technology change and therefore questions of security and information governance. Digital provide a core set of services, which support some common requirements, but we still lack some foundational aspects or capacity to develop our infrastructure in line with changing needs. Some examples of the areas where we would like to do more, but are limited by legacy systems or capacity are as follows:
Mobile device management
NHS email security accreditation
Continuous phishing exercises and education
User profiling for licencing and device requirements

Legacy system replacement
Cyber Essentials accreditation
Role based access control across trust systems
Staff awareness of cyber security and information governance
Asset tracking and physical security of end-user devices
Technical standards assurance for new software application development
Single Sign-On (SSO) and password management solutions
Network segregation to support Internet of Things (IoT) and connected medical devices
Network access control to isolate insecure devices
Port access control for network access

Many of these initiatives would provide additional benefits in addition to providing increased levels of security. It is also true to say that without some of these additional services our ability to deliver more digital services to support care will continue to be limited. These discussions may be progressed through both Digital Assurance Group (DAG).

Incidents Reported to the Information Commissioner
The Information Commissioner's Office (ICO) is the regulator overseeing UK GDPR/Data Protection Act 2018 and Freedom of Information. The Trust maintains a registration as a data controller with the ICO.

Data Breaches are required to be notified to the ICO if they reach a certain level of severity. Within the NHS, incidents are reported via the incident reporting module of the DSPT. Within SHSC, reports to the ICO are authorised by the SIRO following discussion with the Data Protection Officer and the Caldicott Guardian.

During 2023/24, one incidents were reported to the ICO, the ICO was satisfied with the measures we had taken so that no further actions have been required.

The ICO received a number of complaints in relation to processing access to records and undertook an investigation into our compliance with subject access request provisions of the data protection legislation. On completion the ICO informed us on 4 October 2023 that regulatory action is not required in this case. The ICO commented on the robust action plan in place and progress made on the remedial steps taken to reduce the backlog. We complied with the ICO monitoring arrangements and reported significant progress made in April 2024.

Section 6 Caldicott Function

The Caldicott Guardian oversees the use of personal information within the Trust, chairing our information governance group, DIGG, providing advice and acting as a final arbiter on matters of confidentiality.

Caldicott issues are discussed in detail in regular meetings with the Trust Data Protection Officer. The outcomes of discussions are recorded in a Caldicott decisions log and reported to the Digital Assurance Group as necessary.

The majority of the activity deals with matters of information sharing, access to records and record keeping. In considering these matters the Caldicott Guardian and DPO take into account our legal duties, legislation (GDPR), regulatory duties, trust policy and how these decisions should inform changes to policy and practices.

No issues or incidents have been escalated and reported to ARC during the year other than that reported to the ICO.

Some of the examples of the discussions and decisions that are most frequent include:
external requests for identifiable information (e.g. other NHS Trusts, the police, researchers, MPs etc).
data breaches and other incidents involving personal information
recording and use of personal information, including health information, for Trust purposes and external reporting.