BOARD OF DIRECTORS - PUBLIC

SUMMARY REPORT	Meeting Date:	27 September 2023
	Agenda Item:	22

Report Title:	**Data & Information Governance Annual Report (Incorporating SIRO and Caldicott Annual Reports) 2022/23**	
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 Data & Information Governance Group
	Date:	18th April 2023 21st February 2023
Key points/ recommendations from those meetings	A significant proportion of this report is taken from the Data & Information Governance Group: Review of effectiveness 2022/23 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 reporting to Board of Directors in July 2023. The committee noted the negative assurance in relation to: Risk identified re Freedom of Information (FOI) and Subject Access to Records (SARs) and agreed to monitor continue to monitor the position to determine if planned actions have the desired impact. Areas for Improvement included the above risk and Data, Security Protection Toolkit outcome and Information Governance training Compliance to be overseen by the Digital Assurance Group (DAG) The report detailed the new governance structure from April 2023 The duties of DIGG are being discharged to new working groups, overseen by the new DAG, meeting monthly from April. The DAG will report to both the Finance and Performance Committee (for overall digital strategy and technical infrastructure) and ARC (for matters of Information Governance and Cyber Security)	

Summary of key points in report

This annual report from the Data & Information Governance Group (DIGG) 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 DIGG.
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 DIGG 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 Data & Information Governance Group (DIGG) for 2022/23 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 DIGG handled a large quantity of work to fulfil its objectives throughout the year.
- section 2.2 presents third-party reports received by the DIGG.

DIGG 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 assurance.

Areas of improvement 2023/24 - the areas identified are Freedom of Information (FOI) & Subject Access Requests (SARs), Data Security Protection Toolkit outcome and Information Governance training compliance, to be overseen by the DAG.

Current risks – highlighting the concern re. FOI & SARs.

Further to this report detailing the position for 2022/23, the risk re FOI and SARs remains. It has continued to be difficult and time-consuming to review the backlog and work towards compliance. FOI and SARs are now subject to monthly oversight at the Executive Management Team where the recovery plan will be monitored and further mitigation agreed if progress isn't delivered.

We have communicated with the Information Commissioners Office to inform the of our position and seek advice re some mitigation steps who have subsequently requested further information on the position. We responded on the 14th September and await further communication.

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, 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 (BAF risk 0021) risk at the time (subsequently split into two, risk 0021a & 0021b).

Note negative assurance and risk in relation to FOI and SARs significant backlogs.

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

Recover services and improve efficiency	*Yes*		*No*	***X***
Continuous quality improvement	*Yes*	***X***	*No*	
Transformation – Changing things that will make a difference	*Yes*	***X***	*No*	
Partnerships – working together to make a bigger impact	*Yes*		*No*	***X***

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 – KLOE 4,5 and 6
Data Security and Protection Toolkit	*Yes*	***X***	*No*		DIGG 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 DIGG 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*		*No*	***X***	Report relates to review of meeting effectiveness
Organisational Development /Workforce	*Yes*		*No*	***X***	Report relates to review of meeting effectiveness
Equality, Diversity & Inclusion	*Yes*		*No*	***X***	Report relates to review of meeting effectiveness
Legal	*Yes*	***X***	*No*		Effectiveness of the DIGG, through its decision-making and monitoring, provides assurance of our compliance with statutory requirements
Environmental Sustainability	*Yes*		*No*	***X***	Report relates to review of meeting effectiveness

Data & Information Governance Annual Report (including SIRO and Caldicott Annual Reports) 2022/23

Introduction

The structure of the report follows the annual workplan of the Data and Information Governance Group (DIGG). 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 a standard operating procedures for the implementation of Data Protection Impact Assessments (DPIA), Data Processing Agreements (DPA) and Information Sharing Agreements (ISA).

DIGG Dashboard

Dashboard providing 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 DIGG meetings and part of assurance reporting to ARC.

Standard Operating Procedures

Standard procedures are in place for DPIAs, ISAs and DPAs. Over the last year we have established a Data Protection by Design (DPD) log, which 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 DIGG and evidence for the DSPT. assessment.

Over the coming months we aim to fully embed the log and generate summary data to be included in the DIGG dashboard.

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 DIGG 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 2022/23 and decisions taken:

2.1 The objectives listed in the DIGG Terms of Reference were mapped to the DIGG Work Plan for 2022/23, which shaped a standing agenda for key reports at meetings throughout the financial year. The table below provides a chronology of key actions and decisions taken.

Key report	Related key actions/decisions at meetings
DIGG Dashboard (held on Monday.com) Purpose: dashboard reporting: - Information Governance training compliance - Server patching compliance - Windows 10 updates - Phishing Attack incident log - Insight document deletions log - Completion rate of DSPT audit actions	**21/04/2022**: confirmation that DIGG's recommendation to raise the target for Information Governance (IG) training compliance to 95% was endorsed by the People Committee and took effect from 1st April 2022. **21/04/2022**: agreement to keep Insight Document Deletions on a watching brief. **06/09/2022**: agreement that IG Training compliance should be linked to access to systems. **21/02/2023**: DIGG approved the recommended actions and Standard Operating Procedure (including removal of access to systems in certain circumstances) to achieve higher levels of IG Training compliance and endeavour to meet the DSPT requirement of 95%.
Data Protection Impact Assessments (DPIAs), Information Sharing Agreements (ISAs) & Data Processing Agreements (DPAs): highlight report Purpose: for assurance	**24/06/2022**: approval of the DPIA for Sheffield Teaching Hospital's request to access Insight. **21/02/2023**: DIGG acknowledged that work with Sheffield City Council on the DPIA for the disaggregation of social workers is ongoing and was assured that challenges are not anticipated.
Information Governance Policies: update report Purpose: to seek input	**21/04/2022**: DIGG approved the process for access requests to records held by Sheffield Archives – with the process being incorporated into the Records Management Policy. **21/04/2022**: DIGG supported granting external access to Insight to a group of staff at Sheffield Teaching Hospitals

	24/06/2022: the Chair connected DIGG's discussions re. the Recording Policy to the Mental Health Legislation Committee's discussions about the use of CCTV in relation to Human Rights. The Data Protection Officer (DPO) and the Human Rights Officer have since collaborated on a draft CCTV policy.
Data & Information Incidents: highlight report Purpose: for assurance	**24/06/2022**: DIGG agreed that the Phishing Attack June 2022, warranted escalation to ARC. **31/10/2022**: DIGG was informed that one incident was reported to the ICO via the DSPT reporting tool. **13/12/2022**: DIGG was informed that the ICO issued a decision that no further action on their part was necessary. **13/12/2022**: DIGG agreed that the Phishing Attack November 2022, warranted escalation to ARC but was assured by the speed of response to minimise the impact. **21/02/2023**: In response to an assessment of the November Phishing Attack, DIGG supported the DPO's recommendations to update the Confidentiality Code of Conduct statement and agreed that a full audit of compromised accounts should not be undertaken as it would not be proportionate response to the level of risk.
Data & Information Risks: presentation of the Digital department's Directorate and Corporate Level risks Purpose: for assurance and to invite challenge	**24/06/2022**: confirmation that the registered risks re. the storage of paper documents at Fulwood and clinical records at President's Park, were transferred to the Leaving Fulwood Project and were no longer DIGG's responsibility. **31/10/2022**: DIGG supported a proposal to split BAF0021 into two risks – 'Cyber' and 'Digital Systems'. DIGG accepted the Board's levels of risk appetite (low for cyber, moderate for digital systems). **21/02/2023**: DIGG was informed that ARC approved of the new BAF risks.
Freedom of Information & Access to Records: performance report Purpose: for assurance	**06/09/2022**: confirmation that the FOI & Access to Records function was moved into the IMST (now Digital) department. **31/10/2022**: DIGG acknowledged that the FOI & Access to Records function is an area of concern. **13/12/2022**: DIGG was informed that there is low confidence in historic FOI & SARs data and weaknesses have been found in the processes. ARC alerted of concern via an AAA report to the January '23 meeting. **21/02/2023**: DIGG informed that ARC has escalated concern to the Board. DIGG received the FOI & SARs performance report (including findings from a validation exercise on FOI & SARs received within the last 12 months) and acknowledged the stark picture it presented. DIGG supported colleagues to take proactive measures to improve the situation. DIGG agreed that ongoing significant concern should be escalated to ARC via an AAA report to the April meeting.
Data Security Protection Toolkit (DSPT) Improvement Plan and Audit Actions: progress report	**06/09/2022**: DIGG received the DSPT Audit Report (see item 2.2). **October 2022**: a summary of the DSPT Audit Report was sent to ARC.

Purpose: for assurance and to report progress	**21/02/2023: DIGG acknowledged that a keen watch on the level of IG Training compliance is required if we are to meet standards for submission of the DSPT end of June 2023.**
Data & Information Security Reports: Penetration Test Reports and Remediation Plans **Purpose: for assurance and to**	**06/09/2022: DIGG received the annual Penetration Test Report and the associated Remediation Action Plan (see item 2.2).** **21/02/2023: DIGG was assured that all high and medium**
Annual Report **Purpose: for assurance**	**21/04/2022: agreement that the DIGG Annual Report would incorporate both the SIRO and Caldicott Guardian's reports.** **July 2022: the DIGG Annual Report was sent to ARC.**

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

2.2 The DIGG received the following:

Meeting	Action plan or 3rd party report received	Provider

06/09/2022	**Data Security Protection Toolkit Final Report, July 2022**
	• Audit assessed the effectiveness of the Trust's data security and protection environment. Outcome:
	  ○ Veracity of self-assessment = high
	  ○ Assessment against National Data Guardian Standards in scope = Moderate
	• Audit actions were merged with the DSPT improvement plan for reporting progress to DIGG.
	• DIGG was assured by good progress and understood that the retirement of Insight will provide the next significant step on the improvement journey.
		360 Assurance

06/09/2022	**Annual DSPT Penetration Test Report, June 2022** • Annual Penetration Test on the Trust's IT infrastructure as per DSPT requirement. • All externally facing critical and high vulnerabilities were addressed and completed as priority. All medium level remediations have been completed. Low risk remediations are near completion and do not pose concern.	Armadillo Sec Ltd

Summary of key issues of note expected before the end of the financial year:

2.3 The DIGG meeting on 21 February 2023 was considered the last. A proposal to re-establish the Digital Strategy Group as the Digital Assurance Group (DAG), and to dissolve the DIGG, was supported by DIGG members. The duties of DIGG are being discharged to two separate working groups – 'Information Governance' and 'Data Quality' – who will send summary assurance reports to the DAG. The DIGG acknowledged that it is vital that the organisation does not lose grip on data and information governance during the transition phase.

Section 3: Areas of improvement

3.1 Ways to improve the quality of papers were routinely considered at meetings and authors were responsive to suggestions. A review of the DIGG Terms of Reference in October 2022 led to the addition of 'Clinical Operational Lead' to the membership to promote organisational wide ownership of information governance and security.

3.2 Ongoing areas of improvement:

- DSPT toolkit and overall outcome to achieve standards met by 30th June 2023
- Information Governance training compliance to achieve 95% by 30th June 2023 - an Information Governance recovery plan was shared with DIGG members on 21st February 2023, outlining the current position and key actions to recovery. This is being tracked through the Information Governance Group and the DAG
- Development and implementation of the FOI and SARs recovery plan – a recovery plan has been in place since December 2022 and managed via Monday.com. It was presented to DIGG members via a paper on 21st February 2023.

3.3 New governance structure, April 2023 onwards:

- The duties of DIGG are being discharged to new working groups, overseen by the new DAG, meeting monthly from April.
- The DAG will report to both the Finance and Performance Committee (for overall digital strategy and technical infrastructure) and ARC (for matters of Information Governance and Cyber Security)
- The DAG Terms of Reference will be submitted to a future ARC meeting to seek formal ratification.

Section 4: Current risks

4.1 DIGG is reporting 2 key issues to ARC:

- ongoing concern re. FOI & SARs
- current inability to report on all data and information related risks within the organisation.

DIGG is keen to highlight ongoing concern regarding the FOI & SARs position. The significant backlog of requests exposed by a validation exercise has increased concern and the matter is being escalated to ARC as an alert for a second time this financial year (see separate DIGG AAA report to ARC, April meeting).

The Trust's risk register (Ulysses) does not provide functionality to search for risks by theme (for example 'data and information') across the organisation. The Data & Information Risks presented at DIGG are those sitting within the Digital directorate (formerly known as IMST), or those escalated to the Corporate Risk Register from the Digital directorate. It is possible that data and information related risks within other directorates have not been seen by DIGG.

Past discussions with the Trust's Risk Team and Ulysses concluded that searching for risks by theme across directorates was not possible. The Information Governance Manager is revisiting the matter with the Corporate Assurance Manager. This is the starting point for further understanding what is/isn't possible within Ulysses. It is anticipated that, once visible, all Data & Information Risks would be tabled at new sub-groups reporting to the DAG.

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 DIGG and Digital Strategy Group (DSG).

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 2022/23, 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.

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 Data & Information Governance 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.