Proud to care in Sheffield

NHS
Sheffield Health and Social Care
NHS Foundation Trust

Public Board of Directors
Item number: 30
Date: 30 July 2025

Confidential / public	Public
Report Title:	**SIRO & Caldicott Guardian Report**
Author(s)	Chris Reynolds, chief digital information officer
Accountable Director:	Phillip Easthope, senior information risk owner (SIRO), executive director of finance and digital Dr Helen Crimlisk, Caldicott guardian, medical director
Presented by:	Chris Reynolds, chief digital information officer
Vision and values:	The Trust vision is to ensure **we work together** for service users. Digital systems allow patient and staff information to be shared and analysed securely to improve clinical decision making to ensure **we keep improving**. We provide equitable access to digital services to all our stakeholders and specific reasonable adjustments when requires, ensuring **we are inclusive**, and **we provide respectful and kind** care.
Purpose:	The report explains the role of the SIRO and Caldicott Guardian and gives an overview of work that has been undertaken in the last 12 months. This report provides an overview of the activities of the Senior Information Risk Owner, the Caldicott Guardian and the management of information risk and sharing in SHSC. It provides assurance that data and cyber security and information risk is being effectively managed
Executive summary:	In the last twelve months there have been significant improvements in information management and cyber security at SHSC. The governance has been amended so that this important area can be given the focus it needs. A bi-monthly group now meets that reports to ARC. There is a specific risk on cyber security on the corporate risk register, and we are currently drafting one for Artificial Intelligence. Last year the IG manager and her team, recovered the position on Subject Access requests. An internal audit on our DSPT self-assessment was exceptionally good with one low risk item identified. Our cyber security continues to improve. We have completed all actions on last year's penetration test and clarified the scope for this year's test. Additionally, we have used capital funds to invest in products that improve our remote security (zscaler), upgraded data centre software and undertook a tabletop exercise to identify improvements that can be made in our response to a major cyber incident. The growing market of Artificial Intelligence is causing a significant amount of interest from suppliers who are well funded and looking to sell products into the NHS. We have setup a group to consider these developments and approve any tools that may be useful to us.

Which strategic objective does the item primarily contribute to:					
Effective Use of Resources	**Yes**	X	No		
Deliver Outstanding Care	Yes		No		
Great Place to Work	Yes	X	No		
Reduce inequalities	Yes		No		

What is the contribution to the delivery of standards, legal obligations and/or wider system and partnership working.	
Increasingly digital clinical systems are used to share patient information to deliver outstanding care. With the introduction of Rio, we will have the ability to take part in the Shared Care Record and provide a Patient Engagement Portal. We have a legal responsibility to share information in the interests of providing care to our patients and to keep patient and staff information secure and private. We take part in partnership working by securely sharing patient information to dashboards and for analysis by the ICS and the provider collaboratives. This requires technical work underpinned by useful information governance and cyber security.	
Board assurance framework (BAF) and corporate risk(s):	There is currently one corporate risk associated with this item: 5401 - There is a risk that all corporate and clinical services cannot operate safely because technology is unavailable due to a cyber security incident **BAF risk: 0021B**: There is a risk that adequate arrangements are not in place to sufficiently mitigate increased cyber security and data protection incidents
Any background papers/items previously considered:	Audit and Risk Committee 14 July 2025 – the committee approved removal of this annual report as it is now reported through to the committee regularly through the Information Governance, Cyber and Artificial Intelligence Group
Recommendation:	The Boad of Directors are asked to: • **Note** the contents of the report • **Approve** removal of this paper from the work programme as AAA reports now go regularly to ARC which cover in more depth everything in this report.

Proud to care in Sheffield

NHS
Sheffield Health
and Social Care
NHS Foundation Trust

Public Board of Directors

Report title: SIRO & Caldicott Guardian Report

Date of meeting: 30 July 2025

1. Purpose of the report

This report provides an overview of the activities of the Senior Information Risk Owner, the Caldicott Guardian and the management of information risk and sharing in SHSC. It provides assurance that data and cyber security and information risk is being effectively managed.

2. Background

The role of the SIRO at SHSC is to "own the Trusts Information risk policy and risk assessment process" (IMST 003 - Data and Information Security Policy Version 3). This policy sets out the security requirements for all data and information systems in the Trust.

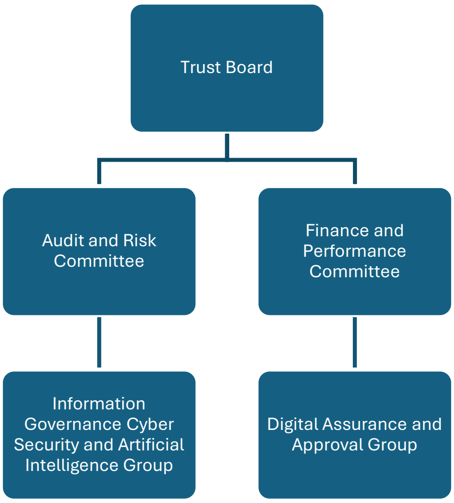
The role of the Caldicott Guardian is to be "responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing" (IMST 003 - Data and Information Security Policy Version 3)

During the year 24/25, Dr Helen Crimlisk became the Interim Medical Director and Caldicott Guardian for the Trust, following the departure of Dr Mike Hunter.

In 2024/25 a review was undertaken of Digital governance. The group (including Information Governance Manager, Data Protection officer, Chief Digital Information Officer, Chief Clinical Information Officer, Chief Nursing Information Officer, Senior Information Risk Owner, Head of Technology Services) concluded that the governance structure should be amended in line with the growing need for senior leadership to consider the growing complexity of Information Governance, Cyber Security and Artificial Intelligence.

It was concluded that a new T2 Group was required to discuss these issues in full. This group drafted a Terms of Reference, which was approved by the Audit and risk committee. The group has been meeting since the 8th of August 2024 and is jointly chaired by the Senior Information Risk Owner and the Caldicott Guardian.

The diagram below shows this reporting structure:



Trust Board

Audit and Risk Committee

Finance and Performance Committee

Information Governance Cyber Security and Artificial Intelligence Group

Digital Assurance and Approval Group

The Group has provided regular AAA reports to the Audit and Risk Committee.

There is a risk on the Board Assurance Framework 0021B: “There is a risk that adequate arrangements are not in place to sufficiently mitigate increased cyber security and data protection incidents.”

There is a risk on the Corporate Risk register 5401 – “There is a risk that all corporate and clinical services cannot operate safely because technology is unavailable due to a cyber security incident.”

Since bringing together IG and FOI requests into a single temporarily funded team in 2023, a signficant backlog has been dealt with (this was reported to ICO and the resulting investigation was satisfactorily closed in 2024).The success of this approach has been built upon with an excellent internal audit of our DSPT toolkit submission, significant assurance and control for subject access requests and sharing agreements, timely policy reviews, expert management of our relationship with the ICO (several incidents reported and managed), good improvements to cyber security as a result of the penetration test action plan and investment in more precise remote monitoring tools.

Additionally, we now have good governance and assurance on our approach to artificial intelligence solutions, despite the lack of investment.

3. Information Governance and Risk Management

The Information Governance function is located within the Digital Directorate. It currently consists of an Information Governance Manager, Data Protection Officer and Information rights team leader. The team of information governance and rights staff underneath this structure, are a mixture of part time and bank. During 25/26, we will be investing in this team to ensure we secure the long-term ability to perform this work.

The team is responsible advising the Trust on how to manage strategic and operational information risk in the organisation, responding to Subject Access requests (requests from third parties and patients for their clinical record) and Freedom of Information Requests. Responding appropriately to SARs and FOIs are legal responsibilities.

The senior members of the team also: collate the Data Security Protection Toolkit (a yearly submission); work with services to draft Data Protection Impact Assessments / Information Sharing Agreements for new and existing services, systems or novel ways of working; collaborate with the IT team with cyber security work; lead communications with the Information Commissioners Office and other external bodies (NHS E, ICS); review incidents raised by operational teams; and work with internal auditors where required.

During 24/25 we reviewed and approved the following policies:

- Data & Information Quality Management
- Data & Information Sharing including E-Mail
- Password Policy
- Data & Information Security

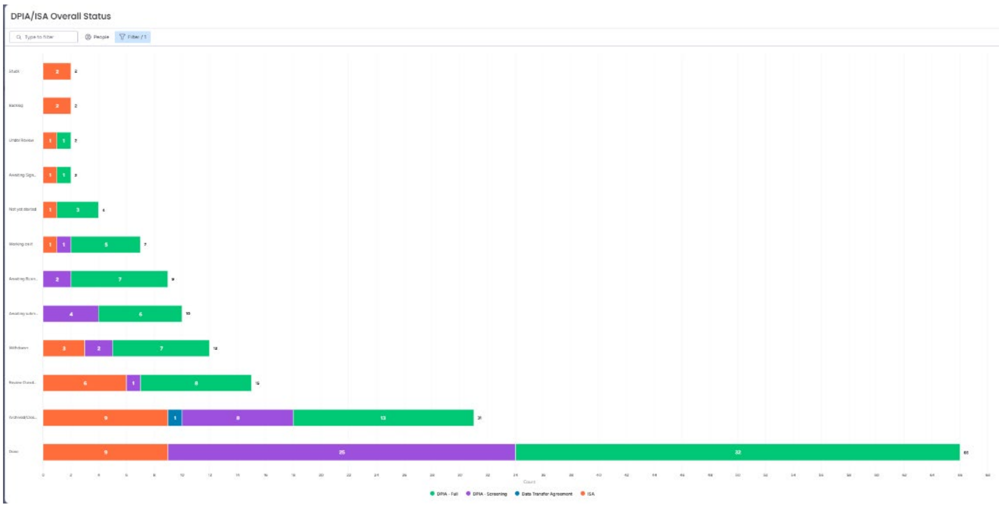
These policies were subject to minor amendments

A key part of managing information risk is to ensure that all staff have appropriate training. At 27th June, 87% of staff had completed their online IG training. There is no national target. We have a local target of 90%.

Information risks are raised through projects, improvement work and incidents. These are discussed and documented with the support of the senior leaders in the IG team and are presented and monitored at the IG Group. There are six IG risks that are currently being managed and mitigated.

4. Data Protection Impact Assessments and Information Sharing Agreements

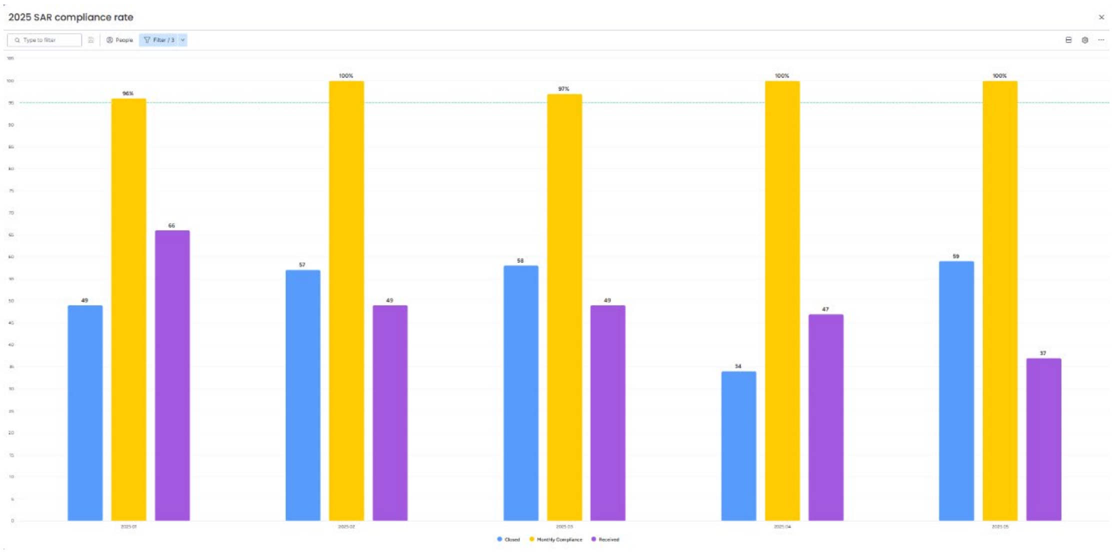
The team are currently managing a workload of one hundred and twenty Data Protection Impact Assessments and Information Sharing Agreements. These range from a DPIA that covers the transfer of staff information to STH to provide the occupational health service to our staff, data sharing to support the use of chatbot for patient recorded outcome measure in Rio and the disposal of hard drives for our printing estate,   This is a maturing picture and as the organisation improves its digital maturity these will become better quality. The line graph below shows the status of these types of agreements:



5. Subject Access Requests

The management of Information Right Requests is difficult and requires a significant amount of effort by the central team (to extract data from clinical records and redact information that is not pertinent to the request) and clinical teams (who have oversight of the record to ensure all information is present and that the clinical risk of sharing distressing information is managed)

The graph below shows our continued excellent performance in this area where we regularly achieve the target of completing 95% of requests within a calendar month. The graph shows the performance each month since the start of 2025, the yellow column is the % performance, the purple is the absolute number of request made in the month, and the blue column is the number of requests closed within that month. (The legislation states that a request should be actioned within a calendar month. So, a request made on the 1st of February should be completed by the 1st of March.)



6. Data Security and Protection Toolkit

The DSPT is a self-assessment undertaken by the IG manager with support from internal colleagues. For additional assurance, the internal auditors conducted a review of a subset of the metrics to check our own self-assessment. This review produced one single action that was low risk for the trust to consider.

For the toolkit, trusts are not expected to have achieved all the objectives. For the self-assessment we submitted on the 30th June, we exceeded expectations for three items, met expectations for forty one and did not meet expectations for three items:

- A3.a (asset management)
- B2.d (identify and access management)
- E4.a (managing records)

As part of our submission, we have provided an action plan for these items, and we expect our status to be “Approaching Standards” once NHS E has reviewed. This item was approved at the IG group meeting in June 25.

Information Governance Training for trust was 86.27% on 27th May 2025. There is no target specified in the national submission and internally we have retained a target of 90%.

7. Externally reportable incidents, changes to practice and internal incidents

Since August 24, the following incidents have been reported to the ICO:

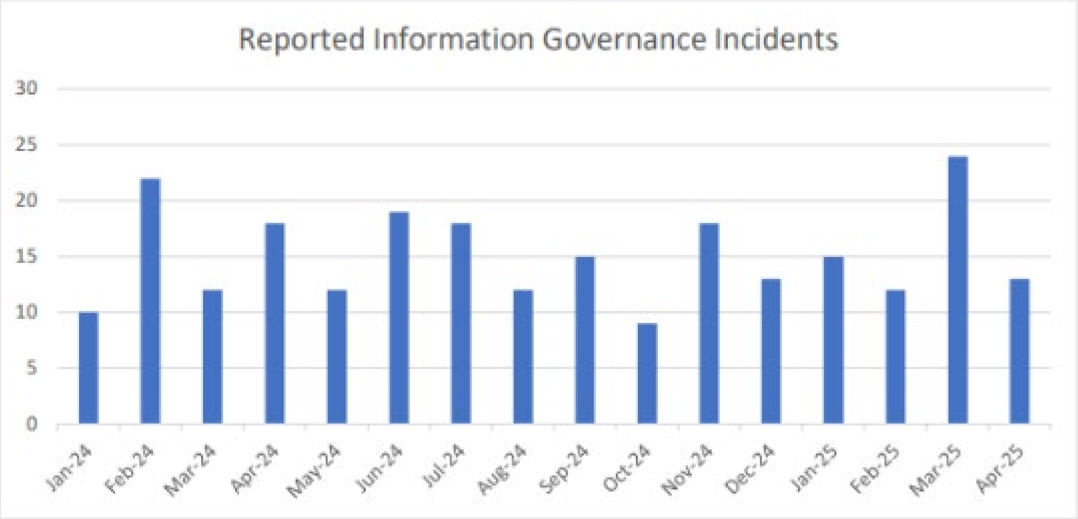
- A service user reported that their records had previously been accessed inappropriately by a member of staff and information shared without their consent. This incident was in a service where we work closely with an external provider Rethink. We have received a report from Rethink, and this is being reviewed by Patient Oversight Safety Panel.

- A service user claimed that staff at a particular service routinely accessed records about people who had not been referred to them - An audit trail for the specific service user did not reveal unauthorised access so the ICO decided not to take further action. We have reinforced our responsibilities for confidentiality with staff in the service.

- A letter containing confidential information which was sent to a service user’s previous address – this was investigated thoroughly by digital and clinical services. The incident arose due to poor operational practice (staff not checking addresses in Rio) compounded by the Rio Data migration. Reports and briefings have been shared with the IG and Cyber group, Clinical Executive Safety Design Group, Senior Leadership Team, Executive Management Team and Trust Board.

  In the Insight patient record it was custom and practice to use aliases when treating staff. In Rio, a patient's record is linked to national demographics which includes their name. This allows patient records to be linked together across organisational boundaries with confidence. After consulting with Senior Leaders, and IG and Cyber group we decided that we would take the opportunity to ensure a holistic record is available to staff and removed the need for the use of aliases.

All services have an excellent maturity to reporting incidents. The number of incidents reported by staff is shown in the table below:



The newly established second tier group, is assured each month by a report that deals with specific themes. The peak within March is within the normal range. In the June report, we were assured that action had been taken to assist services with misfiling clinical records, the inappropriate use of WhatsApp to share patient information, and the legacy of the liquidation of Real World Health.

8. Cyber Security

The IG, Cyber Security and group manages and mitigates the corporate cyber risk: **5401** - “There is a risk that all corporate and clinical services cannot operate safely because technology is unavailable due to a cyber security incident”.

To mitigate this risk, we have taken the following actions:

- Conduct annual DSPT internal audit with Audit 360
- Scope of Penetration Test has been agreed
- Tabletop Cyber Incident Exercise took place in June. The participants explored how an outage to the rostering system would affect the operation of the Trust

- We have invested in and implemented a zero-trust security product that improves our security and the user experience
- The 2024 Pen test recommended we upgrade the software in our data centre. We have invested in this

The monitoring of further actions will go through this Group.

The group monitor the following areas regularly through a report from the IT Operations Team Lead:

- NHSE Cyber Alerts – we are advised by NHSE on weaknesses to software and hardware products when they arise. We are requested by NHS E to report to them whether we use the specific product. If we do not, we report we do not use it. If we do use it then we follow the mitigation they recommend

- Infrastructure Patching Compliance Status – As part of our agreement with Microsoft we regularly issue patches to the windows operating system and the office suite of products. This is monitored nationally to provide assurance and includes our Windows 11 Rollout Update Status

9. Artificial Intelligence

There has been significant investment by commercial software companies in artificial intelligence solutions. This is causing pressure on NHS organisations who are being heavily marketed to. Often these solutions are built on freely available large language models (Chat GPT, Copilot). As part of the governance of the trust, we have agreed that the IG, Cyber Security and AI group, will be the group that authorises the use of these tolls in our environments. The group will consider the clinical safety, information governance and cyber threats and benefits these tools present. Because of the open nature of these tools, we are conducting an internal communications campaign to advise staff on the policy of the organisation.

Additionally, we have completed an initial free pilot of MS Premium with administrative staff and are following this up with a paid (£720 for 25 licences) to test how we can use these tools to achieve better quality meetings.

We have deployed already two tools: A redaction tool used by IG, to assist with Subject access requests and a chat bot to enable patients to complete Patient Reported Outcomes. We expect these to provide better patient engagement with PROMS and a quicker service when processing subject access requests.

10. Looking forwards

In 25/26, we expect to improve our cyber security by ensuring we have in place a dedicated role, who will be supported to keep up to date with all aspects of cyber security. We are investing in the establishment of the information rights team that is currently made-up a of a diversity of bank and other short-term employments. We have not significantly invested in Artificial Intelligence support so we expect to adopt technologies as pilots and then explore how we might support them.

We are drafting a plan to support managers to understand their responsibilities as the owners of Information Assets. This will include a course that is already available on ESR and improve the overall management of information.

As usual we will have a Penetration test, which will identify weaknesses in our infrastructure that we will then draft an action plan to remediate

The provision of a report of this nature is an overhead for the team that is out of alignment with standard practice. We already provide AAA report to ARC and update the Annual Report. We would request that this additional workload is stood down.

1. Recommendations

The Board of Directors are asked to:

- **Note** the contents of the report
- **Approve** removal of this paper from the work programme as AAA reports now go regularly to ARC which cover in more depth everything in this report.