# BOARD OF DIRECTORS - PUBLIC

| SUMMARY REPORT | Meeting Date: | 28 September 2022 |
|---|---|---|
| | Agenda Item: | 24 |

| | | |
|---|---|---|
| **Report Title:** | **Data & Information Governance Annual Report (Incorporating SIRO and Caldicott Annual Reports) 2021/22** | |
| **Author(s):** | Andrew Male, Adam Handley, John Wolstenholme & Julie Eckford | |
| **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 |
| | **Date:** | 26 July 2022 |
| **Key points/ recommendations from those meetings** | To provide a summary view of our overall cyber security position.<br><br>Audit & Risk Committee were assured by the report and in particular the position regarding Information Governance requirements, specifically in relation to the Data Security & Protection Toolkit (DSPT) risk governance and noted the plans to address where current standards are not yet met.<br><br>The committee noted the negative assurance in relation to Freedom of Information (FOI) and Subject Access to Records (SARs) and agreed to monitor the position to determine if planned actions have the desired impact. | |

**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 which meets every two months.

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.

**Recommendation for the Board/Committee to consider:**

| Consider for Action | | Approval | | Assurance | x | Information | x |
|---|---|---|---|---|---|---|---|

Assurance against Information Governance requirements placed on the Trust, particularly by the National Data Guardian (NDG) standards.

To be informed of the plans to address areas where we do not meet the NDG standards through implementation of the criteria defined by the Data Protection Security Toolkit (DSPT)

To be informed of the actions required to adopt a more strategic approach to information governance and cyber security in the future.

To provide assurance on our overall cyber security position and the improvements planned for DSPT submission in June 2023. Our current self-assessment shows that we comply with three of the ten standards and have a realistic plan in place to achieve full compliance by June. Our current status shows sustained improvement and is the best position we have seen for compliance to date.

| **Please identify which strategic priorities will be impacted by this report:** | | | | |
|---|---|---|---|---|
| Covid-19 Recovering Effectively | *Yes* | | *No* | |
| CQC Getting Back to Good | *Yes* | ***X*** | *No* | |
| Transformation – Changing things that will make a difference | *Yes* | ***X*** | *No* | |
| Partnerships – working together to have a bigger impact | *Yes* | | *No* | |

| **Is this report relevant to compliance with any key standards?** | | | | | **State specific standard** |
|---|---|---|---|---|---|
| **Care Quality Commission Fundamental Standards** | *Yes* | | *No* | ***x*** | |
| **Data Security and Protection Toolkit** | *Yes* | ***x*** | *No* | | *NIS regulations 2018, GDPR 2018* |
| **Any other specific standard?** | | | | | |

| **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 and Experience | *Yes* | ***x*** | *No* | | Security of patient data and service availability for critical clinical systems. |
| Financial (revenue &capital) | *Yes* | ***x*** | *No* | | Expansion of our capacity and services would require additional investment |
| Organisational Development /Workforce | *Yes* | ***x*** | *No* | | Improvements to mandatory training compliance levels and improved awareness of cyber security and specifically phishing. |
| Equality, Diversity & Inclusion | *Yes* | | *No* | ***x*** | NA |
| Legal | *Yes* | ***x*** | *No* | | Enforcement action or financial penalties in the event of cyber security incidents is a possible outcome under GDPR or NIS regulations. |
| Sustainability | *Yes* | | *No* | ***x*** | NA |

# Data & Information Governance Annual Report (including SIRO and Caldicott Annual Reports) 2021/22

## 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

Over the last year a dashboard has been developed and the data presented as a substantive item at every meeting of DIGG. The dashboard includes data on our server and endpoint patching status, information governance training compliance, progress on audit actions and document deletion incidents. The board can be accessed by members of DIGG between meetings and a snapshot is provided for every meeting as part of the governance record.

### 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 Quality Group (DQG)

The first meeting of the new DQG took place this year and its Terms of Reference (TOR) have been approved by DIGG. The purpose of the group is:

- To provide assurance to DIGG on all aspects of data quality standards for service users and staff and electronic systems that data is stored within.
- To provide a forum to discuss performance against data quality standards, audit, and ad hoc requirements across a range of SHSC activities.
- Coordinate action plans and report progress to improve data quality and information reporting across the trust.

- Ensure data reporting and dataset returns are agreed, kitemarked, version controlled and validated to ensure consistent data quality standards mandated by NHS and commissioning authorities.

At this time, we have concerns about our ability to fully establish this group and bring together those who can contribute to its aims and work. This is something for DIGG to consider in forthcoming meetings.

## Data and Information Risks and Incidents

There are five data and information risks at corporate level in addition to the Board Assurance Framework (BAF) risk 0021. These 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.

Due to significant work over the last year on retiring of legacy systems and improvements to patching compliance it has been possible to lower the current risk rating for the BAF risk and risk 4121 to 12 from 15. The following table provides a brief update on the position for the BAF risk and the five corporate level risks.

| Risk Ref | Summary | Progress Made and Future Actions |
|---|---|---|
| BAF.0021 | There is a risk that the reliance on legacy systems and technology leads to increasing network or system downtime and cyber security incidents;<br><br>caused by historic system issues requiring complex maintenance, inadequate system monitoring, testing and maintenance, cyber security weaknesses, further development of legacy systems and delays in the procurement and roll out of replacement system;<br><br>resulting in patient safety and clinical effectiveness being compromised by a loss of access to key clinical and administration systems and data protection incidents | With the progress that has been made to retire old systems and the controls that provide very good recovery from Insight document deletion incidents, the likelihood score has been lowered from 4 to 3 given a current score of 12.<br><br>Two criteria have been set for reduction of the severity score:<br><br>1. Achieving 'standards met' for DSPT<br>2. Full retirement of Insight in Q1/Q2 2023<br><br>Neither of these criteria will be met in 2022. The current action on this risk to make improvements on DSPT and sustain them is to increase staff resource for focused work on it on a continual basis. |
| Corporate 4121 – linked to BAF risk. | There is a risk to patient safety, caused by key clinical documents being deleted, resulting in clinical decisions being made with incomplete or limited information and potential delays to patient treatment, e.g., missed appointments. | A range of tools and supporting procedures are in place to identify when this occurs, the documents to be restored, the users involved and clinical impact. These processes are working well and is monitored at each meeting of DIGG. These improvements have supported the decision to lower the likelihood score from 4 to 3 |

| | | |
|---|---|---|
| | | giving a current risk score of 12.<br><br>As with the BAF risk the score is unlikely to be reduced further until Insight is retired. All feasible actions have been implemented, but the situation is actively monitored at each meeting of DIGG. |
| Corporate 4612 | There is risk that system and data security will be compromised caused by IT systems continuing to be run on software components that are no longer supported resulting in loss of critical services, data and inability to achieve mandatory NHS standards (Data Protection Security Toolkit). | While we continue to be reliant on some legacy components due to Insight very good progress has been made in other areas. Email services have been migrated to a supported platform (apart from Insight dependencies) and legacy servers have been fully retired.<br><br>The criteria for reduction of the current risk score of 9 includes retirement of Insight, paying for extended support for a component of Insight while in service and external security validation of our email infrastructure. |
| Corporate 4483 | There is a risk that trust IT systems and data could be compromised as a result of members of staff providing personal credentials and information upon receipt of phishing emails received. | While we have reiterated messages on this subject, we know that they have limited impact. We planned to procure a dedicated phishing simulation and training platform to make improvements in this area but have been unable to progress this.<br><br>Plans are being formed to run another one-off exercise, which is likely to show similar, unacceptable, levels of susceptibility to phishing. Only with sufficient levels of staffing to run continual exercises and training or ability to procure and run a platform will we be able to reduce the risk.<br><br>It should be noted that one of the most frequent 'attack vectors' for major cyber security is IT accounts compromised through phishing. |
| Corporate 4545 | There is a risk that staff are not compliant in Information Governance and IT security training as the current mandatory training policy target deadline is set within 90 days from the start of employment in post. This results in staff using trust computer systems without the correct level of information security, information governance and cyber security awareness. This also impacts on the trust not being able to meet the Data | The trust target has been increased to 95% in lined with the DSPT requirement and the deadline for completion decreased to 5 days. However, compliance has fallen steadily since the start of the year to 83% in April.<br><br>Communications have been cascaded from Execs and the training team have been sending out targeted comms to individuals to improve the position and the most recent position has seen an improvement to 85.6%. |

| | | |
|---|---|---|
| | Security Protection Toolkit (DSPT) requirement of 95% trust wide compliance. | As part of our DSPT submission, made in June, we were able to report a compliance level of 91% as the highest level achieved in the last 12 months. Targeted messaging is continuing with the aim of achieving the target as soon as possible. |
| Corporate 4480 | There is a risk that Insight will become increasingly unstable and functionality restricted by continual development of the system, which is built on some obsolete and unsupported software components resulting in poor performance, higher chances of failure, increased support and maintenance overheads for IMST and limitations with the trust adhering to NHS Digital and legislation standards including NHS Digital DSPT, Cyber Essentials and NIS. | Presentations to our service leaders and commissioners have taken place to set expectations about development can and cannot be taken forward on Insight with a view to limiting activity to only absolute essentials.<br><br>We are maintaining a watching brief on this and if we can maintain this position the likelihood score could be reduced from 3 to 2.<br><br>This risk will be eliminated once Insight is fully retired. |

## Information Governance Policies

The following policies have been updated and presented to Policy Governance Group (PGG) over the last year. The main areas of change are highlighted for each policy.

**Data and Information Security** – a general review of the policy took place in March, no significant updates were required, minor updates were made to reflect governance, organisational and technology changes since the last review of the policy. Roles were clarified and updated based on Trust practice and references to national guidance and legislation were updated.

**Remote Working & Mobile Devices** – the policy was updated in April to reflect changes to the Data & Information Security Policy and amendments were made to support hybrid working arrangements. An important change to note is that staff or sub-contractors based overseas permanently are not provided with SHSC equipment and alternative arrangements for access to IT facilities are required through consultation with IMST.

**Passwords** – this policy has been updated for submission to PGG in July. Updates include the addition of multi-factor authentication (MFA) to support deployment of this additional security measure over the coming year and technical measures to prevent the use of insecure passwords. We have considered increasing the minimum length of passwords but have deferred this decision for now, we have therefore set the review point for the policy for the end of year at which point the policy will be updated with the final decision.

A CCTV policy has been in development and presented to DIGG to ensure that the correct practices are in place and in line with data protection legislation, however it was decided that a better approach would be to expand the existing recording policy. DIGG has requested clinical input and review of the changes before the updated policy is submitted to PGG.

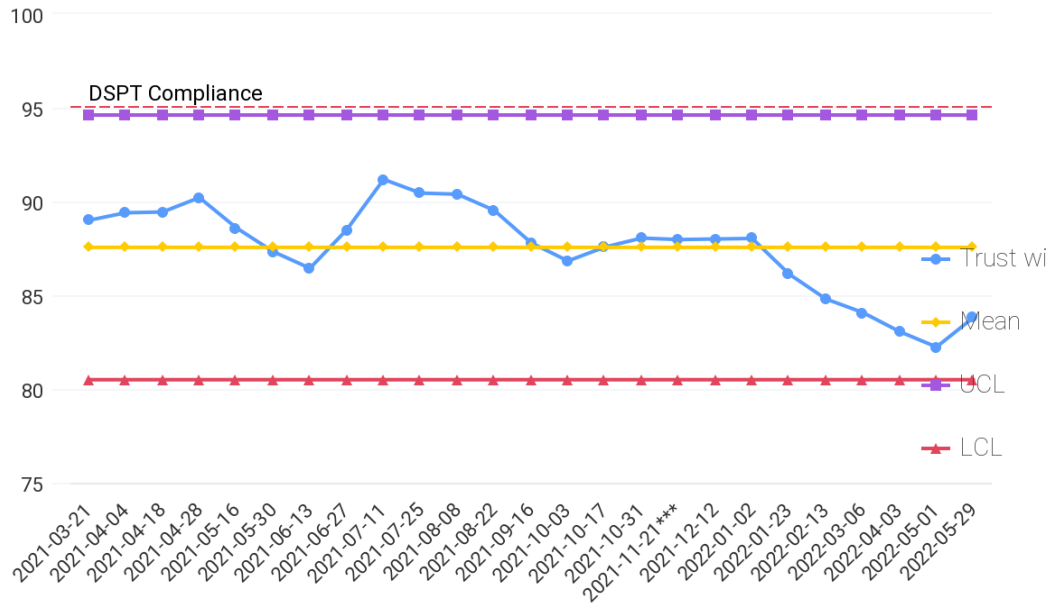
Other Information Governance Policies remain in-date and will be amended in response to audit outcomes or in line with their review dates. Many of these policies were provided as supporting material for our DSPT audit and as such the areas falling under the scope of the audit have recently been scrutinised.

**Safe use of Information Technologies**

Data, Information Security Awareness Training

The trust target for Information Governance, Data Security and Awareness training has been updated to 95% this year to support compliance for DSPT. Over the year training compliance fell to a low of 83%, but with recent communications from Exec and targeted emails to those not in compliance we have seen an increase to 85.5%. The training team are continuing to track compliance and send emails to individuals. It seems unlikely that the target will be achieved for the DSPT submission at the end of June, but with the new target in place should be achievable within the calendar year.

The graph below shows the trend of mandatory training compliance over the year, with the blue line representing the percentage of staff in compliance.




Training needs analysis

An annual review of information governance training needs is included in the DIGG workplan, but this has not taken place to date. A review of the last analysis will be undertaken and information from other Trusts will be used to compare our approach. This will be presented to DIGG before the end of the calendar year.

## Audits

### Penetration Test

Trusts are required to run an annual penetration test of IT infrastructure each year as part of DSPT requirements. Our last penetration test focused on Insight in response to the document loss incidents that were reported to the ICO at the end of May 2020. This year the scope of the test returned to a standard penetration test, looking at our external, internal and Wi-Fi infrastructure and systems. The scope agreed for the test simulates how a cyber-attack could be conducted from outside our network, without compromised user credentials.

The penetration test findings were received at the end of June, the remediation plan was approved by the SIRO. With this approval we can submitted this assertion of our DSPT assessment on 30th of June as 'met'. A report on the penetration test will be presented to the next meeting of DIGG and an update included in the next escalation report to ARC.

### Backup review

NHSX mandated that all trusts should undertake a fully funded review of their backup arrangements citing that inadequate and poorly tested backup arrangements have exacerbated the serious impact of ransomware attacks on several organisations recently. The review was conducted in February and the report was received in April. The scope of the report was based on National Cyber Security Centre guidelines. Verbal update was presented to the June meeting of DIGG with the detailed actions to be overseen by a local group in IMST (Information Security Group) and updates reported to DIGG. Overall, the review showed in four of the five areas we are meeting the guidelines. The one area where we are not meeting the guidelines deals with access control to backups and is a priority for the action plan.

### Data Security Protection Toolkit (DSPT) audit

An audit of our self-assessment against DSPT was conducted in May with the draft report received in mid-June, with the overall assessments being:

- Veracity of self-assessment: **High**
- Assessment against National Data Guardian (NDG) Standards in scope: **Moderate**

The veracity rating shows that our self-assessment against the Toolkit does not differ or deviates only minimally from the independent assessment by 360 Assurance. This provides good assurance that we understand our position and the requirements of the toolkit, but does not mean that we meet all of the criteria set out in the toolkit. Our overall position for DSPT is covered in detail later in this report.

The assessment against NDG standards of moderate shows that there are no standards rated as 'Unsatisfactory', and one or none rated as 'Limited'. Of the 10 standards, 8 were found to be classified as substantial and 2 as moderate, with 2 medium level risks identified, which results in the overall risk assessment of moderate.

### Clinical Coding Audit

The annual clinical coding audit was commissioned as part of the DSPT requirements. The audit found that the Trust had exceeded the required standards of data quality for inpatient diagnosis coding and had met the standard for training of the coder.

## Freedom of Information (FOI) and Access to Records

It has been a difficult year in the administration of access to records[1] and freedom of information (FOI) requests due to staffing issues within the Corporate Affairs team: a lack of permanent staff and under resourcing. The permanent member of staff left in the summer of 2019 and since then there has been a high turnover of agency staff and periods where no staff have been dedicated to these functions. A backlog of requests built up and there was inconsistency in the processes followed and poor record keeping. The team currently comprises three agency staff. Since August, a member of staff with knowledge of the relevant legislation has been in post and has provided oversight of Access to Records since November. An experienced administrator has been working on access to records since January. This has provided an opportunity to develop processes, improve record keeping, get requests back on track, and address the backlog.

[1] Includes subject access requests and other requests for patient information such as service to service requests, e.g. requests from NHS Trusts, Court orders, the Coroner, requests for records and / or reports from the Police and other agencies such as the Criminal Injuries Compensation Authority.

Access to records has improved significantly since January: record keeping has improved, documentation has been refined, the process for allocating records for review via the Head of Service has resulted in more timely responses, an update to the software has enabled records to be extracted more easily, staff are asking for and being provided with advice.

FOI processes and record keeping have improved, but performance is not consistent due to not being able to recruit and retain staff with suitable skills. Since January there have been four FOI administrators. Further work needs to be done on processes and engagement with staff who respond to requests to elicit more timely responses with information that has been quality assured within the service providing it. Responses are frequently returned to services due to the poor quality or inadequacy of the response, which would not be appropriate to send to the requester.

In response to the current position a summary report was presented at April DIGG providing a service overview of Information (FOI) and Subject Access Requests (SAR) processes, performance, and resources. The report concluded that additional resource was required to ensure our ability to respond to FOIs and access to records could be improved and sustained.

Performance information for the year is as follows:

## Freedom of Information (FOI) requests

| Request type | Quarter | Requests received | Open requests | Completed ≤20 working days | Completed >20 working days | On hold | Withdrawn |
|---|---|---|---|---|---|---|---|
| FOI | Q1 | 103 | 56 | 2 | 45 | 0 | 0 |
| FOI | Q2 | 82 | 22 | 36 | 20 | 4 | 0 |
| FOI | Q3 | 103 | 18 | 27 | 51 | 6 | 1 |
| FOI | Q4 | 123 | 28 | 79 | 10 | 5 | 1 |
| **Total** | **Q1-Q4** | **411** | **124** | **144** | **126** | **15** | **2** |

## Access to records requests

| Request type | Quarter | Requests received | Open requests | Requests completed ≤30 days | Requests completed ≤90 days | Requests completed > 90 days | On hold | Closed requests[2] |
|---|---|---|---|---|---|---|---|---|
| Access to Records | Q1 | 117 | 7 | 25 | 32 | 30 | 0 | 23 |
| Access to Records | Q2 | 133 | 22 | 47 | 27 | 9 | 1 | 27 |
| Access to | Q3 | 94 | 13 | 40 | 14 | 9 | 8 | 10 |

[2] Requests where the individual no longer requires their records or has not responded to a request for ID; requests that are not subject access requests.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Records | | | | | | | | |
| Access to Records | Q4 | 119 | 26 (14 >90 days;7 < 90 days) | 41 | 15 | 4 | 12 | 21 |
| **Total** | **Q1-Q4** | **463** | **68** | **153** | **88** | **52** | **21** | **81** |

## Data Security Protection Toolkit

The DSPT submission deadline has now been changed to the end of June each year. A great deal of work has taken place over the year to improve our security infrastructure and practices, but our submission this year remains that we do not meet all the mandatory criteria giving an official status of 'approaching standards'. During the recent audit we confirmed our own assessment that some criteria have not yet been met and unfortunately that others could not be assessed as compliant after closer inspection.

The following table presents the DSPT criteria, which we have assessed as not meeting along with a commentary and actions for making progress towards achieving the standard. The actions will be discussed and monitored by DIGG.

| Evidence item reference | DSPT evidence item text | What actions do you plan to take to meet the requirement? |
|---|---|---|
| 1.1.8 | A data quality forum monitors the effectiveness of data quality assurance processes. | The first meeting of the forum has taken place, but until fully established we cannot confirm that we meet the criteria. There is a current issue in establishing the forum resulting from insufficient capacity and competing priorities. |
| 3.2.1 | Have at least 95% of all staff, completed their annual Data Security Awareness Training? | Compliance as of mid-June stands at 85% indicating that the 95% target will not be achieved this year. In April the Trust target has been updated from 80% to 95%. Non-compliant staff have been contacted directly and communications cascaded from our Execs to their teams. Trust reporting for all mandatory training is shared with teams every three weeks and their position against the target highlighted. |
| 4.3.1 | All system administrators have signed an agreement which holds them accountable to the highest standards of use. | This was identified as an action in our last assessment but has not yet been put in place. System administrators to be issued with formal responsibilities including those outside of the central IT function. |
| 4.2.4 | Are unnecessary user accounts removed or disabled? | During the audit a sample of leavers in February showed that on average accounts took 75 days to be closed. We agreed that this does not meet the criteria and subsequently investigated the processes involved. As of April, a new notification process from HR to IT has been put in place and |

| | | |
|---|---|---|
| | | we have confirmed accounts are being closed in good time. We will therefore submit the criteria as met in our submission and the final audit report will also reflect this as agreed with 360 Audit. |
| 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. | As a result of not meeting the criteria for 9.3.1 (OWASP security vulnerabilities) we cannot meet the criteria for 4.5.4 as one of the vulnerabilities in our EPR is how system level passwords are stored. This criteria cannot be met until Insight is retired. |
| 6.2.11 | You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult. | DMARC and DKIM configuration is in place but is not blocking emails that do not pass the policies due to a third-party finance solution not having their DMARC and DKIM configuration in place. IMST are working with the provider to configure the correct details so this issue can be resolved. All configuration is in place and the system is currently set to monitor traffic against policies, but not to enforce them. |
| 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, and signed off by the SIRO. | Ongoing work programme to replace IT systems or software including the new EPR Programme. This criterion also brings desktop software into scope and currently a proactive process is not in place to meet the criteria. A new post has been created in IT to provide additional capacity to undertake the necessary work. |
| 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. | As agreed through DIGG, reluctantly, we have accepted the risks present in our current EPR with the implementation of a new system the route to addressing these risks. |

In our last annual report, we outline the intention to put in place a cyber security programme, but while an outline case was put together, our resources were then diverted to other activity. The decision was therefore taken to prioritise the expansion of IMST capacity in general enabling us to tackle some security initiatives and put the department in a better position to move from a reactive to a more proactive position. Reflections from the recent DSPT audit, that support this decision, is that we achieve good outcomes with limited

resources, but lack the capacity to keep pace with the increasing cyber threat and the expanding requirements of DSPT.

## Governance

Last year an informal group was set up in IMST, Information Security Group (ISG). ISG aims to provide a forum for IMST staff who are most actively involved with information governance and security to review actions from DIGG and audits to be incorporated into work plans. The group has proved to be a useful forum and its work was used as supporting evidence for the recent DSPT audit.

DIGG meetings continue to work well and both the interim and new Director of Corporate Governance have commented on the quality and effectiveness of meetings.

## Overall Cyber Security position

DSPT is a good guide to our overall cyber security position and through our last two audits we have demonstrated that we have a good understanding of our risks, are transparent about our position and despite limited resources, do not have any known critical risks outside of our in-house EPR. However, 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. IMST 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 2021/22, four incidents were reported to the ICO as follows

- The wrong address being recorded against a service user resulting in a letter being sent to that address in error
- A report by a service user that an interpreter had disclosed confidential information about them inappropriately
- A temporary staff member sharing information about a service user inappropriately
- Details of a former carer being given out, resulting in that person being contacted about a service user

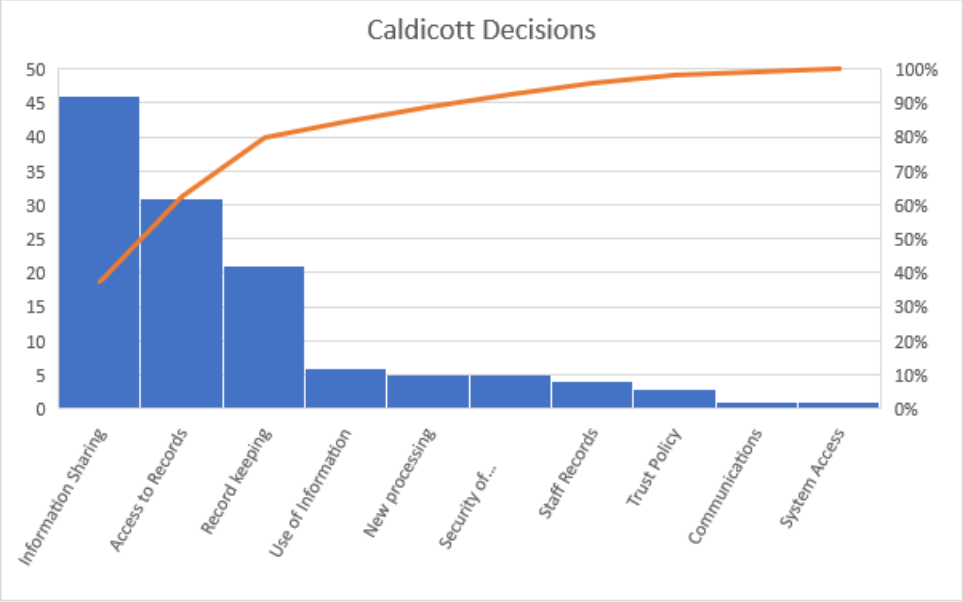
The ICO has considered all these incidents and has been satisfied with the measures the Trust has taken so that no further actions have been required.

## 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 log of discussions and decisions has been further developed over the year and will shortly form part of the dashboard that is reviewed regularly at DIGG.

A snapshot of the requests, discussions, and decisions that the Caldicott Guardian and Data Protection Officer have overseen in the last year is provided in the chart below:




As the chart shows approximately 80% 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.

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

With recent improvements to our recording of this activity and through presentation of this information to DIGG, we will be able to provide increased assurance and have another source of data to inform the work of the group.

## Summary of cyber security position

DIGG use the Data Security and Protection (DSPT) Toolkit, an online self-assessment tool, to measure and publish our performance against the National Data Guardian's (NDG) ten data security standards. The NDG standards are a helpful way to summarise our overall cyber security position. However, to provide a full picture we also need to consider the underlying risks involved in achieving and sustaining the standards. The table in this concluding section outlines the NDG standards, providing a RAG rating for each, defined as follows:

- Red – Some criteria under this standard have not been achieved and risk we will not achieve them for the next DSPT submission
- Amber – Some criteria under this standard have not been achieved, but we are on track to achieve them by June 2023
- Green – All criteria under this standard have been achieved

Alongside the NDG rating is a risk rating based on the cyber security risks that DIGG have oversight for and defined as follows:

- Red – A BAF risk details issues that can be associated with criteria within the standard
- Amber – There are one or more corporate level risks that are associated with criteria within the standard
- Green – There are no corporate level risks associated with the criteria in the standard

Achieving a NDG standard will often have a direct impact on the risk rating, but this may not always be the case. For example, if several critical processes rely on an individual, manual intervention or cannot be continually sustained, we may still see an associated risk score of twelve or above.

## Compliance against National Data Guardian standards

| **People**<br>Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles. | | **Process**<br>Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses. | | **Technology**<br>Ensure technology is secure and up to date. | |
|---|---|---|---|---|---|
| All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes. | | Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals. | | No unsupported operating systems, software or internet browsers are used within the IT estate. | |
| NDG standard 1 | Risk | NDG standard 4 | Risk | NDG standard 8 | Risk |
| All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches. | | Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. | | A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually. | |
| NDG standard 2 | Risk | NDG standard 5 | Risk | NDG standard 9 | Risk |
| All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit | | Cyber attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection. | | IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards. | |
| NDG standard 3 | Risk | NDG standard 6 | Risk | NDG standard 10 | Risk |
| | | A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management. | | | |
| | | NDG standard 7 | Risk | | |

Last year our we had a red rating for three standards (4, 8 and 9), but progress on retiring old systems and the progress of the EPR programme now give us confidence that we will be able to achieve the standards by the next submission in June 2023. Audit actions and the DSPT improvement plan to achieve compliance have been presented to DIGG and will continue to be monitored over the coming months. Overall, we have seen many improvements in the last eighteen months and plans are in place to continue this work with the replacement of Insight having an impact across many NDG standards.