East London
NHS Foundation Trust

REPORT TO THE QUALITY ASSURANCE COMMITTEE
17 September 2020

Title	Annual SIRO report – April 2019 to March 2020
Authors	Chris Kitchener - Associate Director of Information Governance (DPO) Philippa Graves – Chief Digital Officer
Accountable Executive Director	Amar Shah – Chief Quality Officer & SIRO

Purpose of the report

This report provides an overview of the Trust's compliance with the General Data Protection Regulation, the Data Security and Protection Toolkit, and the data and cyber security agenda across the Trust. It provides assurance that data and cyber security and information risk is being effectively managed.

Summary of key issues

The Trust has made significant improvements in data and cyber security compliance over the last year, particularly the last six months of the financial year. The biggest remaining risks to the Trust are asset and data flows mapping plus information governance annual training compliance. Cybersecurity is an area of intense and continued focus, and the Trust is working with NHSD and 3rd party providers to address the ongoing risks, and achieve CyberEssentials + accreditation.

Strategic priorities this paper supports (please check box including brief statement)

Improved population health outcomes	☐	
Improved experience of care	☒	Provides assurance personal information is processed in accordance with the law
Improved staff experience	☒	Increases awareness, confidence and personal responsibility for data handling
Improved value	☒	Minimises the likelihood of regulatory Information Commissioner fines

Committees/meetings where this item has been considered

Date	Committee/Meeting
	None

Implications

Equality Analysis	There is no direct impact on equalities;
Risk and Assurance	Provides assurance that data security and information governance is being effectively managed across Trust services
Service User/Carer/Staff	Increases confidence that information assets are being managed effectively and that staff are aware of their responsibilities in processing information
Financial	There are financial implications regarding Smartcard provision
Quality	There are no quality implications

Supporting documents and research material

a. None

Glossary

Abbreviation	In full
IGSG	Information Governance Steering Group
DSPT	Data Security & Protection Toolkit
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
SIRO	Senior Information Risk Owner
CDO	Chief Digital Officer
FOI	Freedom of Information
CFO	Chief Financial Officer
FBIC	Financial, Business & investment Committee
DPA	Data Protection Act

1.0 Report purpose

1.1 Following the high profile loss of 25 million child benefit records by HM Revenue and Customs in November 2007 and the Government's Data Handling Review, government organisations were required to implement an accountability framework, which included the identification of a Senior Information Risk Owner (SIRO). The SIRO is required to provide assurance of practice, progress and developments in information risk management. This is done through an annual report to the Board. An interim six-monthly report is taken to Information Governance Steering Group (IGSG).

2.0 Structure

2.1 **Deputy Chief Executive - t**he Trust revised its information governance arrangements in November 2019 with Executive responsibility transferred from the Executive Director of Planning and Performance to the Deputy Chief Executive.

2.2 **Senior Information Risk Owner - t**he Senior Information Risk Owner (SIRO) role moved from the Chief Financial Officer to the Chief Quality Officer in October 2019. The post was previously combined with the Caldicott Guardian, but this was a conflict of interest. The SIRO has responsibility for ensuring organisational information risk is properly identified and managed and that appropriate assurance mechanisms are in place. The SIRO must be a senior manager with Board responsibilities. The SIRO acts as an advocate to the Board for information risk, takes ownership of information risk (including policy) and provides written advice on the annual governance statement in respect of information risk.

2.3 **Associate Director of Information Governance and Data Protection Officer (DPO) -** the DPO is a required role under the General Data Protection Regulation and includes raising awareness, overseeing privacy implications for new services and implementing new systems and ways of working. The DPO is available for members of the public to contact directly to raise concerns about privacy. The post holder is supported by a small information governance team. In March 2020

the Registration Authority (Smartcard) function transferred to People and Culture to better align with recruitment processes.

2.4 **Information Asset Owners (IAOs) - t**he Trust's IAOs are locality Service Directors and corporate Associate Directors or functional leads and have a direct reporting line to the SIRO for information asset and data flows management. Information Asset Administrators support the IAOs and are usually managers of a service.

2.5 **Chief Digital Officer (CDO) -** leads both the operational delivery of day to day digital services to the Trust, and the development of new digital solutions, and the technical architecture it sits on, encompassed in the creation and delivery of the Digital RoadMap. They are also the SRO for Cyber Security. The programme of work to deliver digitisation and transformation and lead the Digital First aspiration of the Trust is led by the CDO.

2.6 **Caldicott Guardian - t**he Chief Medical Officer is the Caldicott Guardian and is responsible for ethical decisions relating to disclosure of special categories of information (usually health information) about service users. The Caldicott Guardian is not responsible for decisions regarding disclosure of non-service user information.

3.0 Assurance framework

3.1 **Information Governance Steering Group (IGSG)** oversees and approves data security and information governance matters. The Group works to an annual programme including sponsoring and monitoring the completion of the Trust's Data Security and Protection Toolkit (DSPT) and General Data Protection Regulation (GDPR) / Data Protection Act (DPA) compliance. This includes information asset management, confidentiality incidents, information sharing, access to records compliance, Freedom of Information compliance, data security audit and data security training and awareness. IGSG reports to the Quality Committee quarterly and to Quality Assurance Committee twice yearly.

3.2 **Digital Strategy Board** oversees the deployment of digital technologies including approval of deployment of new / enhanced systems and hardware that underpin the digital transformation of the Trust. The Board is chaired by a Non-Executive Director. It is accountable to the Service Delivery Board and reports to the Financial, Business & Investment Committee (FBIC).

4.0 Audit

4.1 The **Data Security and Protection Toolkit (DSPT) -** requires organisations to have an annual independent information governance audit. This is undertaken by the Trust's internal auditors. This year a sample of five Assertions across two Data Security Standards (Standard 4, Managing Data and Standard 9, IT Protection) was selected covering 33 items of evidence. Four low level recommendations were made. These have been addressed and the audit closed.

4.2 **Clinical coding - t**he Trust's annual independent clinical coding audit took place in March 2020 resulting in a compliance rate of 98% primary diagnosis coding (against a mandatory 85% compliance requirement) and 97% secondary diagnosis coding (against a 75% mandatory requirement).

5.0 Status of organisational compliance

5.1 **DSPT -** During the previous year the Trust was not fully compliant with DSPT. On 31st March 2019 the Trust had declared 85% compliance with 34 out of 40 Assertions completed. There was an action plan to address remaining areas of non-compliance. The remaining areas were addressed by October 2019 when NHS Digital agreed we were fully compliant. Up to February 2020 with only a small amount of Assertions to complete, the Trust would have been on target to declare itself compliant with the 2019 – 20 DSPT by the agreed submission date of 31st March 2020. The COVID 19 pandemic resulted in early March 2020 with NHS Digital deferring the submission date to 30th September 2020. In March the Trust's ICT priorities became realigned to supporting new digital platforms to enable different ways of working during COVID. This resulted in a small delay to the Trust's submission. We were fully compliant by May 2020 when we uploaded our score to the DSPT.

5.2 **CareCert** - the Trust receives regular CareCert notifications from NHS Digital, and applies the security recommendations on a regular basis. The Trust was an early adopter of the Care Cert service and is signed up as a Cyber Accelerator – receiving additional audit and support from NHS Digital to support the Trust's cyber security agenda. The Trust has outsourced Cyber assurance partners such as IT Health and Sophos but urgently needs to expand its Cyber team to match the increasing risk in this critical risk area, and the 24/7 nature of the threat and response. The Trust has also enrolled into other NHSX programmes such as the Microsoft ATP deployment and Windows 10 ensures the Trust has taken appropriate measures given the available funding to address cyber risks. Cyber remains a key threat to the organisation, an area where ongoing focus must be increased with additional resources, structures and systems put in place over the coming year.

5.3 **Freedom of Information (FOI) - f**rom 1st April 2019 to 31st March 2020 the Trust received 362 Freedom of Information requests. 322 were closed during this period. 251 of the 322 were responded to within the statutory twenty working day time frame - 78% compliance with the requirements of the Freedom of Information Act 2000. Full exemptions were applied to 21 requests (7%). A further number had partial exemptions applied. Although the Act is clear that organisations are not required to respond to a request if an exemption can be applied to any part of it, the Trust takes the view that there is a duty to provide assistance to requesters who have a right to ask for their request to be refined. 44 requests were not relevant to the Trust - all were responded to within twenty working days. Considerable effort is often expended in identifying the relevancy of a request prior to an exemption being applied or the request refused. There have been three requests for review. - the information for two of those requests was subsequently released to the requester. The third request for review was subsequently escalated to the Information Commissioner and is referred to in 5.7 below. This request related to a series of questions including serious incidents,

restraints and seclusion where the Trust applied a Section 12 costs exemption. The Information Commissioner upheld the Section 12 application but issued a Decision Notice advising the Trust had failed to provide the requester with sufficient advice and assistance under Section 16 of the Act. As a result the requester was provided with a full breakdown of the costs associated with each question and advised to resubmit the request. Strengthened procedures were also put in place to provide better clarification when a request is refused.

5.4 **Access to records requests** - when GDPR came into force on 25th May 2018 the time frame for responding to requests for personal information reduced to 40 calendar days to one calendar month. Charges for the provision of information were also in most cases abolished. The Trust has a devolved access to records function whereby requests are dealt with locally. This causes some variance in timeliness, completeness and standards of response. This is addressed in part by an access to records lead network, overseen by the Information Governance Manager. A total of 1429 access to records requests were logged between 1st April 2019 and 31st March 2020. 1261 requests were responded to within the time period. Of these 1155 (91%) were responded to on time.

5.5 **Confidentiality and data security breaches - a**ll incidents are scrutinised daily and appropriate action taken including Trust wide communications, individual support and targeted training. Between 1st April 2019 and 31st March 2020 a total of 582 confidentiality or data security incidents were reported. The Trust reports any confidentiality, data security or cyber security incidents via the DSPT incident reporting function, following a pre-determined matrix and set of questions. Between 1st April 2019 and 31st March 2020 a total of three incidents met the serious incident reporting framework. None met the threshold for notification to the Information Commissioner.

5.6 **Complaints to the ICO -** three complaints were made to the Information Commissioner from 1st April 2019 to 31st March 2020. One concerned an access to records request where the parents challenged perceived withholding of information relating to their teenage children. One concerned an adult patient who challenged inaccurate information in her clinical notes together with the decision to send a discharge letter without her consent. The ICO agreed with the Trust's handling in both cases and closed the complaints without requiring any further action. The other complaint concerned the Trust's handling of an FOI request and resulted in a Decision Notice (see 5.7 below).

5.7 **ICO decision notices -** there has been one ICO decision notice. The requester sought information regarding ECT, restraints, seclusion and serious incidents, asking a total of 69 questions. The Trust in response applied a blanket exemption as the response would have taken in excess of 18 hours. The ICO subsequently issued a decision notice directing the Trust to provide some information where the threshold was not met and to set out clearly which combinations of questions could be answered within the time limit, in an effort to be helpful to the requester. The Trust complied but the requester has not refined the request to date.

5.8 **Policies -** a review programme was undertaken throughout the year and policies strengthened to comply with the General Data Protection Regulation where necessary.

5.9 **Information sharing - i**nformation sharing agreements have been regularly reviewed to ensure sharing is current and appropriate.

5.10 **Contracts –** the General Data Protection Regulation requires organisations to ensure their contracts are compliant with data protection law and where necessary there is a Data Processing Agreement clearly setting out how data is managed and processed. Considerable work has taken place to establish communication links and processes between the Commercial Development and Information Governance teams resulting in the identification, scrutiny and approval of 58 contracts and associated Data Processing Agreements.

6.0 Work programmes with an impact on information risk and assurance

6.1 **ICT risk register** - the Trust faces several risks around its IT services and infrastructure. All risks are subject to regular audit and internal action plans to address the ongoing nature of threats. Of note are the risks around:

- Cyber security –skills & capacity/tools to ensure compliance & response – work ongoing to assess suitable approach to address this – high importance
- IT System Health Check by NHS Digital and Dionach
- Infrastructure (datacentre) operations & security risks
- Data network – New secure boundary Firewalls deployed
- Patching and security updates – ongoing – software patching config needs updating during Covid
- Assessing all flows of PID that are occurring across the Trust, particularly following COVID – such as the IoT management and weaknesses in infrastructure of safe delivery of PID containing items.

6.2 **Data security awareness training -** the DSPT requires organisations to demonstrate 95% of its workforce has undertaken data security awareness training and passed a test of comprehension. The Trust achieved this through a combination of e-learning, classroom training and PowerPoint email training.

6.3 **Information asset management -** GDPR and the DSPT require organisations to have identified their information assets, linked their information flows, assessed contractor compliance and generally risk assessed information assets. A considerable effort was made in the previous year to identify assets. This work continues to take place. This year there has been scrutiny of information processed outside of the UK and the location of suppliers in an effort to support Brexit preparations.

6.4 **Business continuity - a**n annual exercise is now a DSPT requirement to ensure Trusts have plans for managing cyber security risks following the WannaCry incident in May 2017. A Trust wide emergency planning exercise took place in March 2020. Exercise Caterpillar focussed on a malicious hacker who managed to infect both clinical systems and payroll functions resulting in staff not being

paid and therefore refusing to attend work. The exercise was well executed with back-up systems and business continuity being put in place.

6.5 **COVID 19 pandemic -** the onslaught of the COVID 19 pandemic required immediate and significant change to working practices. Interim information sharing agreements were put in place to support the safe sharing of information, mechanisms were put in place to securely action Shielded Patient Lists and Privacy Notices were updated to reflect emergency information sharing measures. Arrangements were made to support remote working including advice on the use of digital platforms together with guidance on maintaining confidentiality standards.

7.0 Decisions escalated to the SIRO

7.1 19-20 Cyber security audit was received by the SIRO, and following a subsequent meeting with the Digital Team & CDO present, an action plan was reviewed , and it was agreed to carry out a follow up NHS Digital audit as well as an independent audit on the Trusts new Firewalls , installed in April 2020. The Firewall PEN test was carried out in August and in summary the new Firewalls passed with no High level security issues identified, a much better picture than the previous report due to the hard work of the digital team.
A further decision and any remedial actions required are pending once the results have published and been reviewed in September / October 2020 by the CDO, who will update the relevant committees and SIRO accordingly.
Please note some of these actions took place after the end of the financial year to which the report relates, on the appointment of the Chief Digital Officer.

8.0 Achievements

8.1 **Data Security & Protection Toolkit -** the Trust achieved a Fully Compliant 2019 / 20 DSPT rating ahead of the revised submission date of 30th September 2020 (March 31st, 2020 submission put back for six months to accommodate COVID 19 pressures.

8.2 **Archiving pilot -** over the years there has not been routine review and destruction of records past their recognised retention periods, resulting in contravention of data protection laws and significant unnecessary costs. A pilot was commenced in early 2020 with one supplier (Iron Mountain) looking at a small sample of boxes / files to determine data quality, destruction potential and improved management of retained files. The pilot was not fully completed by the end of the financial year, but early results show potential for streamlining our archiving.

8.3 **Trainee information governance role - s**ince GDPR came into force it has been increasingly difficult to attract high calibre information governance professionals to public services. In late 2019 a secondment opportunity was advertised across the Trust to offer support and training as an Information Governance Manager. This has worked well as it has given an opportunity to someone to embark on a new career with support available via on the job training together with the chance to acquire recognised information governance

qualifications. The information governance team has also benefitted from the skills and knowledge of the Trust the post holder brings.

8.4 **Smartcards -** the Registration Authority (Smartcards) function became part of the new Service Now ICT helpdesk function when it became available, offering a more streamlined and joined up approach to Smartcards and ICT issues. In March 2020 the team transferred to People and Culture. A review needs to be undertaken following the changes that Covid has presented, to ensure it is still compliant. The initial feedback has been positive.

8.5 **Agile working -** A number of services and sites are now adopting the new models of agile working spaces developed in conjunction with East Ham Care Centre and People & Culture. Tower Hamlets CAMHS is in the design phase for their Greatorex Street site and many others are reviewing their desktop layouts by moving to docking stations and laptops. This has been accelerated in the **Covid Response** phase with over 1500 laptops deployed with VPN working numbers rising from 1,800 to 4,000+. Digital have had to scale out infrastructure, secure and expand our use of tools and solutions to mobilise our workforce. Remote working concurrency levels at peak have now increased from 200 to 1,500.
These actions partly relate to the new financial year rather then the year this report refers to.

8.6 **E-Prescribing (ePMA) -** Is a Trust wide transformation programme to implement the WellSky JAC Electronic Prescribing and Medicines Administration system. Which was successfully rolled out across all 52 mental health inpatient wards across 7 sites in London, Beds and Luton during 2019/20. As this is now considered BAU, there is now a dedicated digital & clinical team to ensure support, training and benefits from any upgrades can be leveraged.

8.7 **IT service desk call queue –** A drive to improve the IT ServiceDesk provision and responsiveness saw the average call answer times reduce from 20 minutes (May 2019) to 23 seconds (Feb 2020) and the unanswered call rate (abandoned calls) reduced from 47% (April 2019) to 2% (Feb 2020). This service improvement has been sustained through the challenging increase in demands for support highlighted in 8.5 Covid Response. A large amount of work in achieving this was carried out by the digital team, and continues to be to support the Trust.

8.8 **Windows 10 –** The most recent report from NHSD on ELFT coverage of Windows 10 shows a healthy 96% coverage (8,200 devices of 8,500), with 100% coverage of enhanced support from Microsoft to cover our entire estate. Covid has introduced delays in completing the Windows 10 move, but plans are in place to get to complete coverage during Q3.

8.9 **New Firewalls -** The programme of works to replace our end of life Firewalls and improve our core infrastructure focussed this year on our perimeter security. This work was completed at the end of March with the introduction of the latest generation of Cisco firewalls which will continue to help us maintain a more secure platform and counter-act against new threats in Cyber. Services such as

IPS (intrusion prevention systems) and IDS (intrusion detection systems) have now been switched on.

8.10 **Cloud migration –** A two-year programme of works to retire end of life data centre infrastructure in Alie St (6 years old) and disaster recovery at The Green (10 years old). Migrating all data services into cloud hosted platforms Microsoft Azure and UKCloud. This is a key deliverable in the Trust Digital plan to utilise more secure, scalable and robust IT infrastructure. Currently ongoing. The full benefit realisation and risk avoidance profile of this change will be documented and assessed to ensure governance and tracking of this substantial investment in infrastructure.

9.0 Next year's priorities

9.1 **DSPT -** evidence that is not mandatory this year will become mandatory and will require significant work to robustly provide. We will also be building on the baseline evidence provided this year.

9.2 **Archiving -** continue the work commenced during the Iron Mountain pilot with a view to extending to other archiving providers. This will result in significant cost savings and will ensure better compliance with data protection laws.

9.3 **Deployment of new video conferencing solutions -** Webex, MS Teams, Zoom, AccuRx, Clinic.co and Attend Anywhere are being deployed across the Trust to support virtual staff collaboration, team meetings, corporate events, patient contacts and groups. The adoption of new flexible platforms is essential to continue to offer Trust services in these unprecedented times, however it is important to scale up the digital teams' capability to support this increased deployment and reliance on digital solutions.

9.4 **N365 –** The Trust is committed to the new Office 365 offering from NHS Digital branded N365. This will bring benefits of shared infrastructure, improved end user experience and cost avoidance of c.40% on Microsoft licences. As part of the roll out across the Trust there will be the advantage of removing out of support Microsoft Office 2010 software.

9.5 **Digital Dictation –** Trust wide incremental deployment of a Nuance Dragon Medical One and e-Scription digital dictation solutions.

9.6 **Cloud migration** – Complete migration of remaining servers to the Cloud and retire on-premise systems.

9.7 **New iConnect VPN solution** – a more modern, robust and secure working from home software solution to replace our ageing iConnect remote access.

10.0 Action being requested

10.1 The Board is asked to RECEIVE and DISCUSS the findings of the report