East London NHS Foundation Trust

REPORT TO THE TRUST BOARD: PUBLIC
25 July 2019

Title	Annual SIRO report – April 2018 to March 2019
Author	Chris Kitchener - Associate Director of Information Governance (DPO)
Accountable Executive Director	Steven Course – Deputy Chief Executive and Chief Financial 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 security agenda across the Trust. It provides assurance that data security and information risk is being effectively managed.

Summary of key issues

The Trust has made significant improvements in data 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 continued focus, and the Trust is working with NHSD and 3rd party providers to address the ongoing risks.

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
CIO	Chief Information Officer
FOI	Freedom of Information
CFO	Chief Financial Officer
FBIC	Financial, Business & investment Committee

1.0 Background

1.1 Report purpose

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.

1.2 Senior Information Risk Owner (SIRO)

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.

1.3 Frequency

The Board receives an annual report from the SIRO. An interim six monthly report is taken to Information Governance Steering Group (IGSG).

2.0 Assurance framework

2.1 Information Governance Steering Group (IGSG)

IGSG oversees and approves data security and information governance matters. Its frequency changed this year from bi monthly to every month to ensure robust scrutiny and support. 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) compliance. This includes information asset management, confidentiality incidents, information sharing, access to records compliance, Freedom of Information compliance, data security audit, data security training and Registration Authority functions. IGSG reports to the Quality Committee quarterly and to Quality Assurance Committee twice yearly.

2.2 **Digital Board**

The Digital 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 accountable to the Service Delivery Board and reports to the Financial, Business & Investment Committee (FBIC).

2.3 **Audit**

2.3.1 **Data Security and Protection Toolkit (DSPT)**

The Data Security and Protection Toolkit requires organisations to have an annual independent information governance audit. This is undertaken by the Trust's internal auditors. Following a low rate of Information Governance Toolkit compliance in 2017/18 four quarterly audits were commissioned to provide ongoing scrutiny throughout the year.

2.3.2 **Clinical coding**

The Trust annual independent clinical coding audit took place in January 2019 resulting in a compliance rate of 98% primary diagnosis coding (against a mandatory 85% compliance requirement) and 95% secondary diagnosis coding (against a 75% mandatory requirement).

2.4 **Structure**

2.4.1 **Director of Corporate Planning**

The Trust strengthened its information governance arrangements in May 2018 with Executive responsibility transferred from the Chief Nurse to the Executive Director of Planning and Performance.

2.4.2 **Associate Director of Information Governance and Data Protection Officer (DPO)**

At the same time the information governance function was separated from general governance and risk functions to increase focus and resilience, including the appointment of an Associate Director for Information Governance. The post holder is the DPO. This 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 which also includes Registration Authority (Smartcard) functions.

2.4.3 **Senior Information Risk Owner**

The Chief Financial Officer is the Trust's Senior Information Risk Owner (SIRO) and is responsible for ensuring information risk is effectively managed. The post was previously combined with the Caldicott Guardian but this was a conflict of interest.

2.4.4 **Information Asset Owners (IAOs)**

The 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.

2.4.5 **Chief Information Officer (CIO)**
The CIO leads both the operational delivery of day to day digital services to the Trust, and the development of new digital solutions. The programme of work to deliver digitisation across the Trust is led by the CIO.

2.4.6 **Caldicott Guardian**
The 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 Status of organisational compliance

3.1 **GDPR**
The Trust was not GDPR compliant on 25th May 2018 although it had established its legal basis for processing information, updated its privacy notice and appointed an interim Data Protection Officer. In June 2018 priority was given to establishing an action plan containing fourteen key actions, closely aligned to the DSPT. Of those thirteen actions two (training and asset management) remain non-compliant whilst the remaining eleven have been complied with. There is an action plan to address the two remaining actions – these link closely to the DSPT.

3.2 **DSPT**
The Trust was not compliant with Information Governance Toolkit (IGT) version 14.1 on 31st March 2018, scoring 59%. Sixteen out of 45 requirements were deemed to be non compliant.

The IGT was replaced in 2018/19 with the DSPT, based on ten National Data Guardian standards. The new Toolkit has clear overarching guidelines for evidence provision whilst leaving interpretation more open to organisations than previously. This year not all requirements (Assertions) are mandatory. IGSG therefore took the decision to concentrate on mandatory requirements and to start its evidence base from zero rather than use outdated evidence.

On 31st October 2018 the Trust was compliant with seven Assertions out of a possible 40. On 31st March 2019 the Trust declared 85% compliance with 34 out of 40 Assertions completed. There is an action plan to address the remaining areas of non-compliance.

3.3 **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.
Through our managed service contract with IT Health, the Trust has an outsourced, cloud based threat detection programme in place. This, linked with 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, and an area where ongoing focus must be maintained

3.4 **Freedom of Information (FOI)**

From 1st April 2018 to 31st March 2019 the Trust received 387 Freedom of Information requests. 291 were responded to within the statutory twenty working day time frame - 75% compliance with the requirements of the Freedom of Information Act 2000. Full exemptions were applied to 45 requests (11%). 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. 51 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 two requests for review - the information was subsequently released to the requester'.

3.5 **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 Rights Manager. A total of 982 access to records requests were logged between 1st April and 31st December 2019. Of these 917 (93%) were responded to on time.

3.6 **Confidentiality and data security breaches**

All incidents are scrutinised daily and appropriate action taken including Trust wide communications, individual support and targeted training. Between 1st April and 31st March 2019 a total of 522 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 and 31st March 2019 a total of six incidents met the serious incident reporting framework. Of the six, three met the threshold for notification to the Information Commissioner. All three involved the loss or inappropriate disclosure of special categories of data (health information) about service users. In all three cases the Information Commissioner decided to take no regulatory action against the Trust.

3.7 **Complaints to ICO and ICO decision notices**

3.7.1 **Complaints**

Four complaints were made to the Information Commissioner from 1st April to 31st March 2019. Three concerned responses to access to records requests. One was a data security breach whereby a Trust individual on several occasions emailed

an incorrect recipient. All were investigated and responses provided to the Information Commissioner. None resulted in regulatory action.

3.7.2 **ICO decision notices**

There have been no ICO decision notices.

3.8 **Policies**

A review programme was undertaken throughout the year. To date only the Audio-visual Recording policy remains out of date. All other policies have been reviewed and deleted or updated. A new Data Protection policy has been added to comply with GDPR requirements.

3.9 **Information sharing**

Information sharing agreements are under review to ensure sharing is current and appropriate.

4.0 Work programmes with an impact on information risk and assurance

4.1 **ICT risk register**

The Trust faces a number of risks around its IT services and infrastructure, of particular note are the risks around:

1. Cyber security
2. Infrastructure (datacentre) operations
3. Data network
4. Patching and security updates

All of these risks are regularly subject to audit and internal action plans to address the ongoing nature of the threats

4.2 **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. This was a risk to the Trust given difficulties with OLM at various points in the year. Contingency plans were put in place including classroom training and email presentations. Nonetheless given the high numbers of staff who become non compliant in February and March we achieved 82% compliance rather than the required 95%. An action plan is in place to address this.

4.3 **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. This work had not been started until the appointment of the DPO in September 2018. Although there is was a project to identify and assess assets it was not completed by March 31st 2019. This affects a number of DSPT Assertions and therefore had a high impact on compliance.

4.4 **Business continuity**

A Trust wide emergency planning exercise took place in March 2019. An annual exercise is now a DSPT requirement to ensure Trusts have plans for managing cyber security risks following the WannaCry incident in May 2017. The actions from the planning exercise have been added to those from our ongoing work with

Dionach and IT Health to address security vulnerabilities identified, and will be addressed in our ongoing work plan.

5.0 Decisions escalated to the SIRO

There has not been a need in the last 12 months to escalate any IT related decisions to the SIRO. All audit actions have been undertaken within the IT team.

5.1 Information assets

The Trust considered using an external provider to complete its information assets mapping. This request was discussed in detail with the SIRO and the decision taken to undertake this project in house. Companies approached worked on 'train the trainer' methodology and required the purchase of software that would have required ongoing resource including a system administrator.

5.2 Luton and Bedfordshire Smartcard services

Luton and Bedfordshire services do not have dedicated Smartcard services as the RA Manager attends Luton one day a week. The Trust considered using an external provider. This was escalated to the SIRO for a decision. Following discussion it was agreed the risks of lack of provision did not outweigh the considerable financial resource required. The information governance team will submit a proposal for a limited amount of funding to increase internal resource.

6.0 Achievements

6.1 Information governance

Although the Trust did not achieve full DSPT and GDPR compliance significant progress was made with a final DSPT score of 85% and eleven out of thirteen GDPR requirements satisfied.

6.2 New starter event – London

The information governance team has set up a weekly new starter event in London so that starters receive information governance and RiO training on their first day and are issued with a Smartcard, thereby providing the ability to immediately commence working.

6.3 Smartcards

Significant improvements have been made including morning drop in sessions and access to the IT service desk call queue. This has made it easier to deal more promptly with various Smartcard issues.

6.4 Mobile working

Deployment of over 300 iPads to facilitate improved mobile clinical recording in district nursing teams. The benefits of this deployment have been realised through the improved workspace at East Ham Care Centre, reduced number of desktop PCs required, and savings on office space. A rollout to Mental Health is planned in 19/20, to realise similar benefits.

6.5 ePrescribing

Deployment to Mental Health inpatient units underway, all wards in Tower Hamlets complete with a plan to deploy across the rest of the Trust inpatient units throughout 2019/20.

6.6 **Windows 10**
Rollout across Trust well advanced, due for completion in mid 2019. ELFT will be one of the first Trusts in the country to complete this rollout

6.7 **Bedfordshire community**
Rollout of all Trust systems and IT services was planned by the end of March 2019. This work is complete, the SLA with EPUT has been terminated, and business as usual IT support is now provided to the service.

6.8 **Deployment of new video conferencing service**
Cisco Webex has been deployed in a number of key Trust locations (webex boards) to facilitate meetings, and reduce travel across the Trust geography. This deployment has been successful, and has led to requests for rollout to other Trust locations. Webex is available to staff via apps on mobile devices and laptops, or via a web browser.

7.0 Next year's priorities

7.1 **New starter event – Luton and Bedfordshire**
The intention is to set up new starter weekly events in Luton and Bedfordshire so that new staff based in those localities are able to commence working as soon as possible.

7.2 **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.

7.3 **IT service desk call queue**
The proposal for a new service desk call queue will assist in directing users to the correct team for Smartcard support and will therefore reduce the risk of users being unable to work. The new service desk system went live in April 2019, and will help in managing demand for support services appropriately, including the use of a portal to log requests rather than over the telephone.

7.4 **RiO mobile deployment**
Trust wide deployment of iPads to support mobile working in Mental Health services.

7.5 **Digital Dictation**
Deployment of a new digital dictation solution across early adopting teams. A pilot is currently underway.

7.6 **eObservations**

Replace the current paper based observation process in mental health with an app provided by Servelec for this specific task. This will be made available to appropriate staff on iPads in the 19/20 financial year.

7.7 **Office 365**

Support teams to deliver new ways of working underpinned by the new office suite. A rollout has begun across some early adopting teams (approx. 700 staff), and will accelerate as the deadline for the end of support for Office 2010 approaches (October 2020). The Trust is currently in discussion with NHS Digital regarding the licensing model, and costs to be picked up by the Trust, prior to setting out a business case for adoption.

7.8 **Archiving**

Support teams to undertake a review and subsequent retention or deletion of records reaching potential destruction dates to comply with GDPR and potentially reduce storage costs.

8.0 Action being requested

8.1 The Board is asked to **RECEIVE** and **DISCUSS** the findings of the report.