NHS
East London
NHS Foundation Trust

Senior Information Risk Owner (SIRO)
Annual Report 2020-2021

1.0 Background/Introduction

1.1 Public organisations must have a data security accountability framework including the appointment of a Senior Information Risk Owner (SIRO). The SIRO is required to provide assurance of practice, progress and developments in information risk management. ELFT does this through a bi-monthly Information Governance Steering Group meeting, chaired by the SIRO. The IGSG is accountable to Quality Committee. We take an annual SIRO report to the Board via Quality Assurance Committee and an interim six monthly report to IGSG.

2.0 Progress against workplan during last financial year

2.1 Key achievements

Data Security & Protection Toolkit - 2019 / 20 deadline deferred from 31st March 2020 to 30th September 2020. The Trust achieved a fully compliant rating across all Assertions. Nonetheless the deferred submission date has had an impact on the 2020 / 21 submission which has been deferred from 31st March 2021 to 30th June 2021.

DSPT internal audit - organisations must have an annual independent information governance audit. This year a sample of five Assertions across four Data Security Standards (Standard 6 – responding to incidents, Standard 7 – continuity planning, Standard 8 – unsupported systems and Standard 9 - IT Protection) was selected covering 26 items of evidence. Three overarching recommendations were made covering six points in total. These have been addressed and the audit closed.

Clinical coding audit - the Trust's annual independent clinical coding audit took place in March 2021 resulting in a compliance rate of 98% primary diagnosis coding (against a mandatory 85% compliance requirement) and 98% secondary diagnosis coding (against a 75% mandatory requirement).

Freedom of Information (FOI) – FOI activity remained high throughout the year. There was a slight decrease at the start of the pandemic, resulting in slightly fewer requests than the previous year. 64% were closed on time compared to 78% the previous year, mostly due to changed priorities in directorates during the pandemic. There was one request for review regarding contracts and was subsequently released to the requester. One requester complained to the ICO, resulting in ICO advice to provide support to the requester by advising what could potentially be responded to. This has been done.

Indicator	Previous year (2019 - 20)	Current year (2020 – 21)
Total no. requests received	362	342
Total no. closed	322	299
No. closed / responded to on time	251	191
No. closed / responded to late	71	108
No. where full exemptions were applied	21	30
No. where partial exemptions were applied	Not recorded	30
No. not relevant to the Trust	44	21
No. requests for review	03	01
No. escalated to ICO by requester	01	01

Access to records requests - 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 and is addressed in part by an access to records lead network with regular meetings and training. The number of requests increased slightly this year from 1429 to 1672. 1362 were responded to within the time period. 94% on time. Of note is the significant increase in staff requests, often in response to grievance or other action, all time consuming and potentially litigious.

Indicator	Previous year (2019 - 20)	Current year (2020 – 21)
Total no. SARs received	1429	1672
Total no. SARs responded to	1261	1362
Total no. responded to on time within one calendar month	1115 (91%)	1292 (94%)
No. responded to with an agreed extension of 2 – 3 months	Not recorded	09
No. responded to late	146	70
No. staff requests	05	19

Confidentiality and data security breaches - all incidents are scrutinised daily and appropriate action taken including Trust wide communications, individual support and targeted training. The slight reduction in reported incidents is likely attributed to the start of the pandemic when many individuals were working remotely without full network access and therefore unable to report. 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. Twenty incidents met the serious incident reporting framework. This is a considerable increase compared to the previous year due to changed reporting requirements and a more focussed approach within the Trust. One met the threshold for notification to the Information Commissioner – this was regarding inappropriate access to a patient's record and has now been closed by the ICO.

Indicator	Previous year (2019 - 20)	Current year (2020 – 21)
Total no. data security / confidentiality incidents in period	582	520
Total no. data security / confidentiality 48 hour reports requested	Not recorded	35
Total no, reported to the DSPT	03	20
Total no. subsequently reported to ICO	0	01

ICO complaints / decision notices - three complaints were made to the Information Commissioner. One concerned an email sent to an incorrect address. Another concerned a staff subject access request. 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.
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. The requester did not refine the request but has since submitted a similar one for updated information (still ongoing).

Information sharing - information sharing agreements are regularly reviewed to ensure sharing is current and appropriate. Since April 2020 we have introduced strong governance processes to record information sharing activity. 84 ISAs or third party access agreements have been approved during the year.

Indicator	Previous year (2019 - 20)	Current year (2020 – 21)
Total no. ISAs approved		31
No. new ISAs approved		28
No. existing ISAs renewed		03
Total no. 3rd party access agreements approved		11
No. new 3rd party access agreements approved		10
No. existing 3rd party access agreements approved		01

Data Protection Impact Assessments – DPIAS are required where high risk processing could take place. 50 DPIAS have been completed during the year.

Contracts – contracts must be compliant with data protection law. Where necessary there must be 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 86 contracts and associated Data Processing Agreements compared to 58 the previous year.

Indicator	Previous year (2019 - 20)	Current year (2020 – 21)
Total contracts / DPAs approved – ELFT as Commissioner	39	59
Total contracts / DPAs approved – ELFT as Provider	19	27

Business continuity – the DSPT requires Trusts to undertake **a**n annual exercise based on cyber security risk. This follows the WannaCry incident in May 2017. The Cyber X exercise took place in February 2021 and focussed on ransomware. The exercise was well executed with back-up systems and business continuity being put in place.

Cyber Security - 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, Windows 10 and most recently the NHS Secure Boundary together ensure 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.

Phishing campaign - NHS Digital carried out a simulated phishing campaign in March 2021, 23% (1,019) opened the email and clicked the link, and 3% (133) of the 4,365 staff opened the email and entered their personal credentials compared with an NHS average of 1%. Staff who entered information received feedback and training from NHS Digital after entering their sensitive personal information. NHS Digital will carry out further phishing tests on behalf and at the request of ELFT to improve awareness and correct response.

Cyber security audit - 2020-2021 Cyber security audit was received by the SIRO, 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 in July 2021, the CDO will update the relevant committees and SIRO accordingly. Further to this the Digital Strategy addresses the workforce structure and tools required to deliver a sustainable and secure service provision for the organisation in the face of ever increasing and complex cyber threats.

2.2 What went well, and what learning do we want to share from this?

Archiving – we recognised the historical lack of routine review and destruction of records, resulting in contravention of data protection laws and significant unnecessary costs. We worked with one supplier (Iron Mountain) to assess at a small sample of boxes / files to determine data quality, destruction potential and improved management of retained files. There has already been a small cost saving as we identified 20% of records could have been destroyed, a significant amount several years ago. We also set up local records review processes with Forensics and CHS Newham, resulting in reduced storage costs. Both demonstrate the importance of working closely with and supporting local teams.

Trainee information governance role – we offered a secondment in early 2020 to train someone with good Trust knowledge as an Information Governance Manager. This has proved beneficial and the post holder has been made permanent. We also offered training opportunities to two local Access to Records Assistants who have since taken on enhanced roles as Information Rights Officers, demonstrating the value of developing individuals.

COVID 19 pandemic - 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. Learning points are the ability to respond urgently, think outside the box and maintain data security principles at the same time.

Brexit – all contracts where personal information is processed were assessed to identify where overseas processing takes place, given the lack of an EU Adequacy Agreement and the need to implement new standard contractual clauses. Learning points are the value of working with colleagues (Procurement), the good support given by suppliers, balanced against the need to routinely identify where processing takes place.

Agile working - A number of services and sites are now adopting the new models of agile working spaces developed for example East Ham Care Centre, People & Culture and Tower Hamlets CAMHS Greatorex Street site. As part of the Future of Work many others are reviewing their desktop layouts by moving to docking stations and laptops. This Digital adoption and transformation was accelerated in the Covid Response phase with over 2000 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 tenfold, from 200 to 1,850. An example of digital enabling service continuity is ELFT IAPT services transferred to entirely virtual delivery.

Deployment of new video conferencing solutions - Webex, MS Teams, Zoom (for staff education events), AccuRx, Clinic.co and Attend Anywhere were deployed across the Trust to support virtual staff collaboration, team meetings, corporate events, patient consultations and group therapy and education events. 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. The substantial impact on the network utilisation that will occur when staff return to trust locations is being addressed as part of the network review.

IT service desk call queue – The IT Servicedesk improvements have 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 support the Trust.

Windows 10 – The most recent report from NHSD on ELFT coverage of Windows 10 shows a healthy 100% coverage (9300 devices), with 100% coverage of enhanced support from Microsoft to cover our entire estate.

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. Azure migration has been completed, with 10 servers left to move to UK Cloud. The full benefit realisation and risk governance and tracking of this substantial investment in infrastructure.

Digital Dictation – Dragon Medical One has been successfully deployed across ELFT with a return on investment of over £2 for each £1 spent and clinicians using the auto text function saving an average 30 minutes of time on each day of use. Winscribe has been successfully deployed to replace Bighand creating a closed document creation loop and reducing the risks associated with email transfer of draft clinical documents.

Patient Portal - ELFT worked in partnership with City and Hackney CCG to deploy the patient portal Patient Knows Best and was awarded “Highly Commended” by the Health Services Journal. This improves security of access by patients to their care plan.

PANDO – ELFT successfully deployed the WhatsApp replacement PANDO offering a secure messaging platform to support clinical care.

2.3 What wasn’t achieved, and what have we understood about the reasons for this?

Archiving – although we had intended to roll the project out to other suppliers this was problematic given the pandemic and the issues they faced in accessing records stores during this time

Locality audits – the information governance team routinely visits localities to undertake supportive data security audits. No audits took place this year due to travel restrictions and more pressing priorities for services.

2.4 Any notable risks further to the above

There are four information governance risks currently being addressed:

Information asset registers – if the Trust does not have an up to date information asset register it will not have a record of processing activity and may contravene the GDPR. We are supporting teams to refresh their asset registers.

Subject access requests – if the Trust does not manage subject access requests effectively and respond appropriately, data subjects may complain to the ICO resulting in regulatory action. There is a small consultation underway to create additional resource.

COVID data processing - if the Trust does not have an exit strategy for data processing agreed as a result of COVID it will contravene the DPA and other legislation. All data processing agreements have an end date and will be scrutinised in line with timescales for Control of Patient Information Notices.

DSPT - if the Trust does not comply with the requirements of the DSPT this may impact on the Trust's reputation, result in confidentiality breaches and ICO intervention. 95% training compliance is always a concern and is addressed through a variety of training delivery methods.

Digital risk register - the Trust faces three substantial risk domains around its IT services and infrastructure managed under item 8 of the Board Assurance Framework. All risks are subject to regular audit and internal action plans to address the ongoing nature of threats. Key mitigations include:

Cybersecurity risks

- IT System Health Check by NHS Digital and Dionach
- Patching and security updates – ongoing – software patching config needs updating during Covid
- Skills & capacity/tools to ensure compliance & response – work ongoing to assess suitable approach to address this – high importance

Infrastructure risks (datacentre) operations & security risks

- NHS secure boundary security operations centre
- 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.

ICT governance Risks

- New digital governance structure and processes with the creation of the Digital Solutions and the Digital Operational and Transformation Boards
- Creation of Digital Programme Management Office

2.5 Action taken and planned in response to gaps in implementation or other risks identified

All risks are routinely assessed and actions described above.

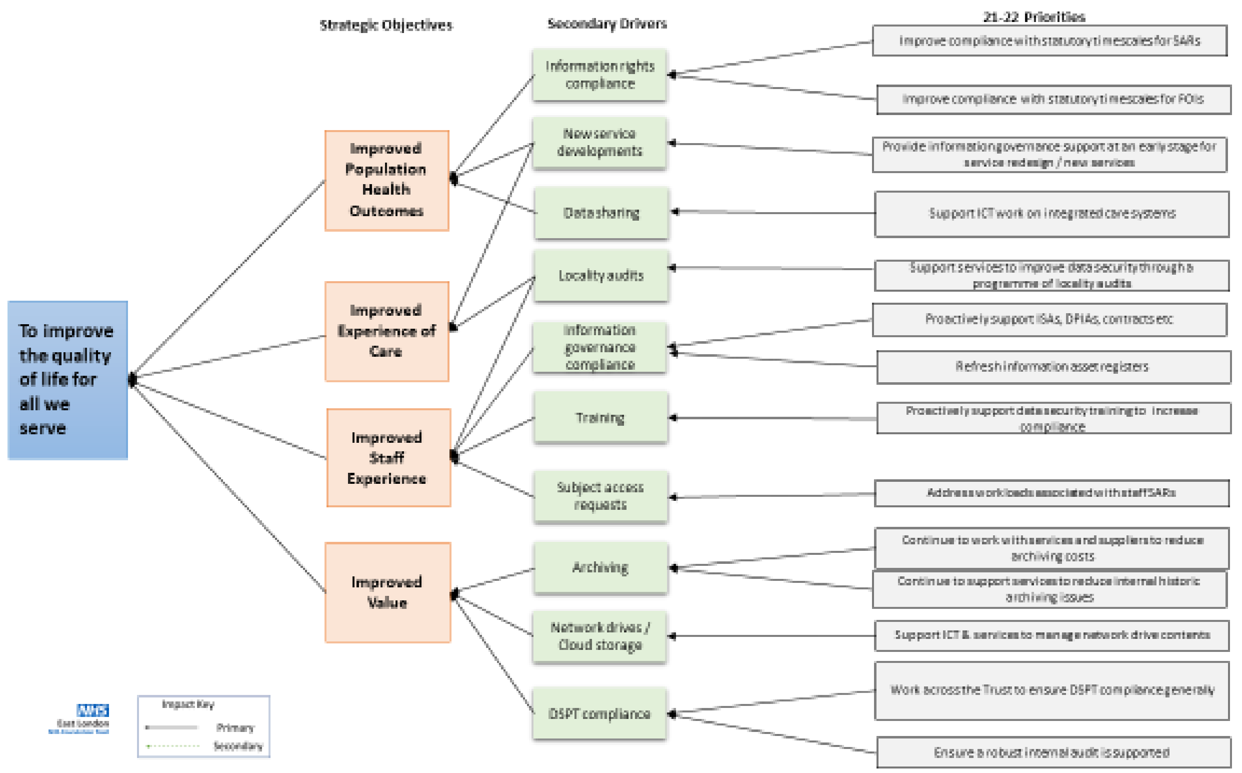
3.0 Workplan for the coming financial year

3.1 IG key priorities

Key priorities are:

- Achieve full DSPT compliance
- Comply with statutory requirements for information rights (FOI and SARs)
- Refresh information asset registers
- Deliver a data security & awareness training compliance programme
- Restart locality audits
- Support archiving projects
- Support network drives / cloud projects
- Support service developments
- Work with partners to support integrated ICT systems

3.2 IG links to Trust objectives


Strategic Objectives
Secondary Drivers
21-22 Priorities
To improve the quality of life for all we serve
Improved Population Health Outcomes
Improved Experience of Care
Improved Staff Experience
Improved Value
Information rights compliance
New service developments
Data sharing
Locality audits
Information governance compliance
Training
Subject access requests
Archiving
Network drives / Cloud storage
DSPT compliance
Improve compliance with statutory timescales for SARs
Improve compliance with statutory timescales for FOIs
Provide information governance support at an early stage for service redesign / new services
Support ICT work on integrated care systems
Support services to improve data security through a programme of locality audits
Proactively support ISAs, DPIAs, contracts etc
Refresh information asset registers
Proactively support data security training to increase compliance
Address workloads associated with staff SARs
Continue to work with services and suppliers to reduce archiving costs
Continue to support services to reduce internal historic archiving issues
Support ICT & services to manage network drive contents
Work across the Trust to ensure DSPT compliance generally
Ensure a robust internal audit is supported
NHS East London
Impact Key
Primary
Secondary

3.3 ICT key priorities

3.4 **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.

3.5 **Cloud migration** – 10 servers holding non-clinical documentation remaining on premise to be moved to UK Cloud.

3.6 **New AnyConnect VPN solution** – a more modern, robust and secure working from home software solution to replace our ageing iConnect remote access by 31 August 2021.

3.7 **NHSX Cyber Security –** run a trust wide cyber education and awareness raising campaign, commission NHSX to rerun a simulated phishing attack, report results to the Digital Strategy Board and include in future SIRO report.

3.8 **Shared Care Records -** Connecting RiO and SystmONE patient records and users to the BLMK ICS Shared Care Record platform.

3.9 **PANDO** – planned deployment of patient care status to improve security and reliability of patient information at hand over.

3.10 **PKB** – deployment across NEL ICS to improve ease and security of patient access to their records and letters.

3.11 <u>What data will we be collecting to understand whether we are progressing against the plan?</u>

An information governance dashboard is routinely tabled at IGSG including:

- ISAs / 3rd party access agreements

- Privacy Officer alerts
- Document removals
- Incidents
- FOIs
- SARs
- Clinical coding
- Training

3.12 How will we report on progress, and adapt the plan as needed in-year?

Information Governance Steering Group – a strategic information governance overview paper is routinely tabled at IGSG and adaptations discussed / approved as necessary.

Ops Group – Ops Group is updated on key issues especially in respect of training compliance.

Quality Committee – receives quarterly updates

Ad hoc groups – relevant items are reported to various groups including Corporate Financial Viability, Heads of Admin, DMTs and specialist working groups.

3.13 Who will be our key stakeholders in delivering the plan, and how will we engage them through the year?

Key stakeholders are staff who will be engaged through the groups set out in 3.4 above, direct contact and regular communications briefings.

3.14 Resourcing requirements or other risks to implementation

Information rights - the information governance consultation will address additional resourcing requirements for processing information rights requests.

Archiving - project resource will be required to support records review work.

Cloud storage / network drives - resource may be needed to support scrutiny and management of network drives pending a move to the cloud