East London
NHS Foundation Trust

REPORT TO THE TRUST BOARD: PUBLIC
25 JULY 2019

Title	Information Governance Compliance – Annual Report 2018-19
Author	Chris Kitchener – Associate Director of Information Governance and Data Protection Officer
Accountable Executive Director	Mason Fitzgerald – Director of Planning & Performance

Purpose of the report

To advise the Board on the Trust's annual compliance with the new annual Data Security and Protection Toolkit, compliance with the new EU General Data Protection Regulation, and to update the Board on continued efforts to improve compliance in this area.

Summary of key issues

The Trust self-declared a Not Satisfactory compliance score of 59% for Version 14 of the Information Governance Toolkit (IGT) on 31st March 2018. The Toolkit ceased to exist on 1st April 2018 and was replaced by the Data Security & Protection Toolkit (DSPT), with a greater focus on information security and is aligned with the requirements of the new EU General Data Protection Regulation (GDPR). All organisations that process personal data were required to be fully compliant when it came into force on 25th May 2018. At that stage the Trust was not compliant.

The Trust took a number of steps to improve compliance in these areas.

On 31st March 2019 the Trust's compliance rating was 85% increasing from an Information Governance Toolkit score of 59% in March 2018. The Trust declared itself 'Not compliant' in March 2019 as it did not meet all standards. Subsequently NHS Digital asked us to submit an Improvement Plan and as a result has regraded our compliance to 'Standards not fully met – plan agreed'.

Similarly compliance with the General Data Protection Regulation increased from three of the thirteen standards being met in May 2018 to eleven being met on 31st March 2019.

For both GDPR and the DSPT non compliant areas related to:

1. Training
2. Asset management
3. Contract management

Our DSPT and GDPR Improvement Plan focusses on these two areas. There is an expectation we will be compliant by August 2019.

Compliance and proposed actions are summarised in this paper. The Quality Assurance Committee will seek assurance during the year.

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

Improved population health outcomes	☐	
Improved experience of care	☒	Provides assurance personal data is processed in accordance with the law
Improved staff experience	☒	Provides a framework and clear guidance on confidentiality for staff
Improved value	☒	Minimises the likelihood of Information Commissioner fines

Committees/meetings where this item has been considered

Date	Committee/Meeting
22.05.2019	Report tabled at Information Governance Steering Group. The report will also be taken to Quality Committee.

Implications

Equality Analysis	This report has no direct impact on equalities
Risk and Assurance	There is a risk the Trust continues to be non compliant with some areas of GDPR and the DSPT. This is being managed through Information Governance Steering Group
Service User/Carer/Staff	There are no direct implications for service users
Financial	Resource is required to achieve compliance
Quality	There are no quality implications

Glossary

Abbreviation	In full
IGT	Information Governance Toolkit
DSPT	Data Security & Protection Toolkit
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IGSG	Information Governance Steering Group

1.0 Background

1.1 The Trust's Information Governance function encompasses data protection, data security, records management, access to records and Freedom of Information.

1.2 The Director of Planning and Performance has executive responsibility for information governance. The Deputy Chief Executive / Chief Finance Officer fulfils the role of Senior Information Risk Owner (SIRO). The Chief Medical Officer fulfils the role of Caldicott Guardian. The Associate Director of Information Governance fulfils the Data Protection Officer role.

1.3 The Board will be aware of the challenges faced in 2017-18 resulting in an Information Governance Toolkit (IGT) score of 59%. An improvement plan was put in place (previously taken to the Board).

1.4 The Data Security & Protection Toolkit (DSPT) replaced the IGT from 2018/19 onwards with a greater and more challenging focus than previously on data security.

1.5 Our 2018-19 baseline DSPT score in July 2018 was Nil. We submitted an interim DSPT compliance score of 17.5% in October 2018.

1.6 In March 2019 our final compliance rating was 85%. We rated ourselves as DSPT 'Standards not met'. NHS Digital invited us to submit an Improvement Plan and subsequently graded us as 'Standards not fully met – plan agreed'.

1.7 It is important to note that whilst some organisations refreshed evidence previously submitted to the IGT, we started the process from the beginning given that information previously submitted had become out of date and in some cases was not especially relevant.

1.8 The Trust also worked on General Data Protection Regulation (GDPR) compliance, increasing compliance from three out of thirteen standards in May 2018 to eleven out of thirteen in March 2019.

1.9 Internal audit carried out quarterly reviews into the Trust's levels of DSPT and GDPR compliance to provide greater scrutiny than previously.

2.0 Data Security and Protection Toolkit (DSPT)

2.1 As stated above, the Trust submitted a final score of 85% on March 31st 2019.

2.2 The Trust declared itself 'Standards not met' (therefore 'Not compliant'). It completed 34 out of 40 Assertions (previously known as Requirements).

2.3 We have an action plan to address areas of non-compliance by end August 2019.

2.4 Five Standards were not met:

- Personal confidential data
- Staff responsibilities
- Training
- Managing data access
- Accountable suppliers

2.5 Within those five Standards there were six non-compliant Assertions:

- Records of processing activities are documented for all uses and flows of personal information
- There is a clear understanding of what personal confidential information is held
- Staff pass the data security and protection mandatory test
- All staff understand their activities on IT systems will be monitored and recorded for security purposes

- The organisation can name its suppliers, the products and services they deliver and the contract durations
- Basic due diligence has been undertaken against each supplier that handles personal information

Each Assertion has specific deliverables, shown below:

STANDARD 1.0	**PERSONAL CONFIDENTIAL DATA**
Assertion 1.4	**Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and DPA 18 Schedule 1 Part 4)**
(1.4.1)	A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied.
(1.4.2)	Have information flows been approved by the SIRO or equivalent local method?
(1.4.3)	Date of when information flows were approved by the Board or equivalent.
(1.4.4)	Provide a list of all systems/information assets holding or sharing personal information.
(1.4.5)	List of systems which do not support individual login with the risks outlined and what compensating measures are in place.
2.0	**STAFF RESPONSIBILITIES**
Assertion 2.1	**There is a clear understanding of what Personal Confidential Information is held.**
(2.1.1)	When was the last review of the list of all systems/information assets holding or sharing personal information?
(2.1.2)	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the SIRO or equivalent local method.
3.0	**TRAINING**
Assertion 3.2	**Staff pass the data security and protection mandatory test.**
(3.2.1)	Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.
4.0	**MANAGING DATA ACCESS**
Assertion 4.3	**All staff understand that their activities on IT systems will be monitored and recorded for security purposes.**
(4.3.1)	All system administrators have signed an agreement which holds them accountable to the highest standards of use.
(4.3.4)	List of all systems to which users and administrators have an account, plus the means of monitoring access.
10.0	**ACCOUNTABLE SUPPLIERS**
Assertion 10.1	**The organisation can name its suppliers, the products and services they deliver and the contract durations.**
(10.1.1)	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.
Assertion 10.2	**Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance**
(10.2.1)	Basic due diligence has been undertaken against each supplier according to ICO guidance.
(10.2.2)	Percentage of suppliers with data security contract clauses in place.

2.6 Within the above Standards and Assertions there are three key remaining areas to address:

- Training
- Information assets
- Contracts

2.7 Training

82% of staff were compliant with their basic data security awareness mandatory training. Although significant effort was made to ensure the required 95% compliance there were a number of setbacks including OLM unavailability for extended periods. Although this was mitigated by classroom and other electronic training formats it undoubtedly had an effect on the final score. We have an action plan to demonstrate 95% compliance by end July. The action plan includes:

- Weekly compliance reporting from the corporate training team
- Bank staff dedicated training days
- Invites for existing staff to attend weekly new starter information governance training
- Programme of locality training
- Email questionnaire completion

2.8 Information assets

There was no action on recording and managing information assets until the appointment of the Associate Director of Information Governance in September 2018. A policy, process and asset template were drafted and approved and Information Asset Owner training rolled out. Whilst a significant number of information asset registers were completed, scrutinised and support given a number of issues became apparent:

- Not every team completed and returned their asset register
- Some teams require further support in meaningful completion of their registers
- Further work is required on contracts

The action plan includes:

- Contact, support and training for teams where asset registers have not yet been completed
- In depth assessment of registers already received and further liaison with services where required
- Establishment of a centralised asset register containing contract details, data flows and records of processing activities

2.9 Contracts

A number of issues were identified during completion of both the DSPT generally and individual asset registers:

- Procurement of systems / software / services directly by teams without information governance or ICT knowledge and support

- Numerous purchase orders set up locally for the same services (mostly archiving providers) instead of one framework contract (therefore data processing agreements do not exist)
- No centralised management of non-clinical contracts therefore obligations under GDPR not met for these contracts

There is an action plan to:

- Assess asset registers for contract information
- Work with the Contracts Manager / Business Development Unit to identify and assess contracts / contractors
- Update or set up framework contracts with data processing agreements

3.0 General Data Protection Regulation (GDPR)

3.1 Preparation for GDPR was led by the SIRO. The Trust took necessary steps prior to 25th May 2018 when the Regulation came into force to establish priorities for GDPR:

- Interim Data Protection Officer appointed pending permanent recruitment
- Established the legal basis for processing information
- Updated its information notices

3.2 Eleven of the GDPR actions have been completed:

Requirement	Implementation date	Owner	Progress
Identify the lawful basis for processing personal data	25 May 2018	DPO	Complete
Review the responsibilities of the Data Protection Officer & ensure an appropriately qualified / experienced person is appointed to the role	25 May 2018	DPO	Complete.
Update privacy notices	25 May 2018	DPO	Complete
Manage subject access requests in accordance with the changes required by GDPR	25 May 2018	DPO	Complete
Update policy & procedures to respect individual's rights	30 June 2018	DPO	Complete
Ensure compliance with more stringent transparency requirements	30 June 2018	DPO	Complete
Update internal processes to comply with the requirement to report specific breaches to the ICO	31 July 2018	DPO	Complete

within 72 hours of becoming aware of a breach			
Ensure that existing & new contracts meet GDPR requirements	31 July 2018	AD Business Development / DPO	Complete
Review compliance with children's rights	31 July 2018	Director Specialist Services / DPO	Complete
Ensure all current & proposed data processing activities have data protection compliant technical & organisational controls in place	31 August 2018	DPO	Data Protection Impact Assessment process for approval at IGSG Information Asset Register / Data Flow Mapping project in progress across the Trust Proposal to complete asset mapping by July 31st 2019
Review how consent is sought, recorded & managed & if any changes are required to comply with GDPR	31 August 2018	DPO	Complete
Manage information risks in a structured way to understand & manage the impact of personal data related risks	28 February 2019	SIRO / DPO	Complete
Ensure there is comprehensive understanding of the information held by the Trust & how it is used	31 March 2019	IG Manager / DPO	To be achieved via new training programme, with 100% compliance expected by 31 March 2019 Compliance shown to be at 82% on 20 March 2019 Proposal to be compliant by 30th June 2019

3.3 Two actions are outstanding, with an action plan:

- Information asset management
- Training

These relate closely to the DSPT action plan.

4.0 Confidentiality breaches

4.1 All confidentiality breaches are reported on Datix, screened, graded and appropriate action taken including training, procedure revision and support.

4.2 The majority relate to minor breaches – emails sent to incorrect addresses, wrong attachments to letters, lost Smartcards etc

4.3 There were three breaches meeting the threshold for reporting to the Information Commissioner's Office (ICO):

- An email was sent out by the Tower Hamlets Recovery College regarding a money management course to what at the time was believed to be a distribution list of 667 service users. The recipients' names were added to the 'cc' instead of the 'bcc' field
- A clinician placed a work notebook containing patient details in his bag and left it on public transport
- The house of a community health team worker was broken into and a bag containing details of 17 patients was taken

4.4 In each of the above three cases an investigation report was submitted to the ICO. In each case the ICO has decided to take no regulatory action.

5.0 Assurance

5.1 The Information Governance Steering Group (IGSG) met bi-monthly from July 2018 – March 2019 and will continue to meet monthly. The Quality Assurance Committee will continue to seek assurance that progress is being made.

5.2 Internal audit provided updates to the Quality Assurance Committee during 2018-19 and will continue to do so.

6.0 Action being requested

6.1 The Board is asked to **RECEIVE** and **NOTE** the report for information