East London
NHS Foundation Trust

REPORT TO THE TRUST BOARD – PUBLIC
11 July 2018

Title	Annual Information Governance Update
Author	Chris Kitchener, Associate Director of Governance & Risk (Data Protection Officer)
Accountable Executive Director	Mason Fitzgerald, Director of Planning and Performance

Purpose of the Report:

To advise the Board on the Trust's compliance with the annual Information Governance Toolkit submitted on 31st March 2018, compliance with the new EU General Data Protection Regulations, and to update the Board on plans for improving 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 as at 31st March 2018. This was because it failed to achieve the required Level 2 for a number of areas, thus automatically generating a Not Satisfactory rating.

The Toolkit ceased to exist on 1st April 2018 and has been replaced by the Data Security & Protection Toolkit (DSPT), published in June 2018, Although there are similarities the DSPT is more information security focussed, and is aligned with the requirements of the new EU General Data Protection Regulations.

The Trust is taking a number of steps to improve compliance in this area. This is summarised in the paper. The Quality Assurance Committee will seek assurance during the year that the Trust is making sufficient progress against the DSPT and GDPR requirements.

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

Improved patient experience	☒	Ensures personal information is robustly managed
Improved health of the communities that we serve		
Improved staff experience	☒	Provides a framework and clear guidance on confidentiality for staff
Improved value for money	☒	Minimises the likelihood of Information Commissioner fines

Committees/Meetings where this item has been considered:

July 2018	This report will also be taken to Information Governance Steering Group and Quality Committee

Implications:

Equality Analysis	This report has no impact on equalities
Risk and Assurance	There is a risk that the Trust is unable to address non-compliant

	areas. This will be managed through new management arrangements together with more frequent internal audit. Assurance is provided through Information Governance Steering Group and Quality Committee
Service User/Carer/Staff	There are no direct implications for service users
Financial	The new Information Governance function requires additional funding.
Quality	There are no quality implications

Glossary

Abbreviation	In full
IGT	Information Governance Toolkit
DSPT	Data Security & Protection Toolkit
GDPR	General Data Protection Regulation
HSCIC	Health & Social Care Information Centre
IGSG	Information Governance Steering Group

1.0 Background

1.1 The Trust's Information Governance function has historically been managed as part of the Governance and Risk department, with line management responsibility with the Chief Nursing Officer. The function is responsible for all aspects of information governance, including data protection, access to records and Freedom of Information.

1.2 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.

1.3 The NHS requires all Trusts to assess compliance with information governance standards on an annual basis, via the Information Governance toolkit.

1.4 The Trust's overall rating was 93% in 2014. In 2016 the overall rating dropped to 74%. There was no increase in 2017. In March 2018 the final score dropped further to 59%.

1.5 Falling compliance rates can be attributed to:

- Increased complexity and more stringent standards over the years, particularly for ICT requirements
- The challenges associated with providing information governance functions to new Trust business
- Difficulties in attracting permanent staff and reliance on interim agency staff

1.6 The Trust has also been preparing for the introduction of the EU General Data Protections Regulations, which came into force on 25 May 2018.

1.7 Internal audit have carried out reviews into the Trust's levels of compliance with the toolkit, and GDPR preparation, and have made a number of recommendations for improvement.

2.0 Information Governance toolkit

2.1 As above, the Trust submitted a final score of 59% in March 2018.

2.2 The Trust's overall compliance rating was 'Not Satisfactory'. Eight Requirements were submitted as Level 1 scores and five as Level 0 scores. Ratings less than Level 2 automatically result in 'Not Satisfactory' however robust the other Requirements may be.

2.3 Many areas of non-compliance in this version are due to policies and procedures not being updated, and therefore cannot be used as evidence.

2.4 The new toolkit for 2018/19 has now been published, and is re-named the Data Security & Protection Toolkit (DPST). The DPST aligns with the requirements of GDPR.

3.0 GDPR preparation

3.1 Preparation for GDPR has been led by the SIRO, with a working group. Preparation has been affected by the lack of/delay in guidance for NHS organisations.

3.2 The Trust took all necessary steps prior to 25 May 2018, namely:

- Appointing the Data Protection Officer
- Establishing the legal basis for processing of information
- Updating information notices
- Revising the subject access requests process

3.3 Work to update policies and procedures is well underway.

4.0 Improvement plan

4.1 Due to concern regarding the Trust's compliance, the executive team have reviewed the arrangements for information governance in the Trust. A number of measures have been put in place to improve information governance compliance:

- Executive responsibility for information governance has transferred to the Director of Planning and Performance to give more focus and align executive responsibilities
- The Data Protection Officer has been appointed to take overall responsibility for information governance, its strategic development and engagement with Trust priorities
- The GDPR action plan has been refreshed in light of the IG toolkit scores, and the requirements of the DPST.
- The Information Governance Steering Group meeting frequency has been increased to monthly for the next six months
- Standard owner meetings have been set up to effectively manage evidence portfolios for the DPST
- Arrangements are being made for quarterly internal audits of information governance (as opposed to previous annual audits) thereby monitoring compliance and identifying weaknesses at an earlier stage
- A new senior role, Associate Director of Information Governance, has been created and is currently being recruited to. This role will include the role of Data Protection Officer.

4.2 The GDPR / DSPT action plan focusses on:

- Information risk
- Information asset management
- Data protection impact assessments

- Contracts
- Confidentiality breach management
- Clinical records audit

4.3 A summary of key milestones is set out below:

Requirement	Implementation date	Progress
Establish an implementation plan for GDPR compliance	25 May 2018	Plan established
Identify the lawful basis for processing personal data	25 May 2018	Complete
Review the responsibilities of the Data Protection Officer & ensure an appropriately qualified / experienced person is appointed to the role	25 May 2018	Complete.
Update privacy notices	25 May 2018	Complete
Manage subject access requests in accordance with the changes required by GDPR	25 May 2018	Practice changed. Policy being updated.
Update policy & procedures to respect individual's rights	30 June 2018	Policy drafted and being submitted to IGSG
Ensure compliance with more stringent transparency requirements	30 June 2018	Policy drafted and being submitted to IGSG
Update internal processes to comply with the requirement to report specific breaches to the ICO within 72 hours of becoming aware of a breach	31 July 2018	Confidentiality breach reporting tool just published. Incident policy under revision. Changes to Datix in progress
Ensure that existing & new contracts meet GDPR requirements	31 July 2018	To be achieved through revision of contracts with the Business Development Unit
Review compliance with children's rights	31 July 2018	To be achieved by review of children's rights by Director of Specialist Services. Unlikely to affect Trust services as we do not offer on line services

Ensure all current & proposed data processing activities have data protection compliant technical & organisational controls in place	31 August 2018	Process being finalised, to be followed by IGSG approval and communications plan
Review how consent is sought, recorded & managed & if any changes are required to comply with GDPR	31 August 2018	To be achieved through review of current clinical systems
Manage information risks in a structured way to understand & manage the impact of personal data related risks	Ongoing	Assurance to be provided through IGSG and SIRO involvement. Policy under revision and communications plan being drafted
Ensure there is comprehensive understanding of the information held by the Trust & how it is used	31 March 2019	To be achieved via new training programme, with 100% compliance expected by 31 March 2019

5.0 GDPR benchmarking

5.1 Internal audit have carried out a benchmarking exercise into organisations' GDPR preparations, which was submitted to the Quality Assurance Committee on 25 June 2018.

5.2 A summary of the Trust's position in relation to the benchmarking is set out below:

Area:	Benchmarking:	Trust position:
1. Are decision makers and key individuals within the organisation aware of GDPR?	20% little/no awareness 53% discussions/awareness 27% GDPR working group	The Trust had set up a working group and has taken papers to the IGSG and Quality Committee. There also also been discussion at Trust Board and sub-committees. Information has been publicised to staff.
2. Do you have documented what personal data you hold, where it came from and who you share it	33% not started to consider 40% considering data mapping 27% data mapping in progress/complete	The Trust has completed data mapping as part of previous information governance audits, and is carrying out more

with?		robust data mapping in line with GDPR
3. Have you reviewed your current privacy notices and put a plan in place for making any necessary changes?	40% no policy in place 47% policy in place/needs updating 13% policy in place/reflects GDPR	The Trust has reviewed its privacy notices and published these on the website
4. Have you checked your procedures to ensure they cover all the rights individuals have?	17% no policy in place 73% policy in place/needs updating 10% policy in place/reflects GDPR	The Trust has a policy in place which is currently being reviewed
5. How will you handle subject access requests in line with the new requirements?	20% no policy in place 57% policy in place/needs updating 13% policy in place/reflects GDPR	The Trust's process has been changed, and the policy is being updated
6. Have you identified the lawful basis for your processing activity, have you documented it and updated your privacy notice to explain it?	25% no policy in place 25% policy in place/needs updating 50% policy in place/reflects GDPR	The Trust has identified the lawful basis and updated its privacy notice accordingly
7. Have you reviewed how you seek, record and manage consent?	40% not yet considered 47% consent process being reviewed 13% consent processes in place	This work is underway and due to be completed by 31 August 2018
8. Are systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity?	60% action to be taken 40% being reviewed	This work is underway and due to be completed by 31 July 2018
9. Are there procedures in place to detect, report and investigate a personal data breach?	43% no policy in place 44% policy in place/needs updating 13% policy in place/reflects GDPR	The Trust has a policy and system in place, which is being reviewed. This is due to be completed by 31 July 2018.

10. Have you considered the guidance on data protection by design and data protection impact assessments?	43% not yet considered 30% discussed and actions in progress 27% in place	The guidance has been considered
11. Have you assigned an officer to take responsibility for data protection compliance?	30% no 70% yes	A Data Protection Officer has been appointed
12. Has the management of third party relationships been considered?	37% not considered 33% in progress 30% considered/policy updated	Work to review arrangements in contracts is underway and due to complete by 31 July 2018.

6.0 Information Governance incidents

6.1 All confidentiality breaches are reported on the Trust's incident reporting system, Datix

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

6.3 There were three reportable breaches to the Information Commissioner in 2017/18. None resulted in any recommendations or sanctions, as the Trust was able to demonstrate that appropriate action had been taken.

- A car belonging to a barrister representing the Trust was broken into and Inquest bundle including staff statements, patient records (patient of SEPTs), Police statements and IPCC report were in bundle of papers. This has been closed by the ICO
- A report was sent to a list of professionals, some external to the organisation, in error. Closed by the ICO

- 29 appointment letters sent to one patient in one envelope. This has been closed by the ICO but remains open under Trust investigation. Similar breaches have occurred and believed attributable to the use of hybrid mail. An external investigator is managing this investigation.

6.4 There are regular Trust wide communications briefings in an effort to highlight the importance of treating confidentiality seriously.

6.5 Going forward, any information governance incidents that are reportable to the Information Commissioner will be reported to the Trust Board as a serious incident.

7.0 Next steps

7.1 The Quality Assurance Committee will seek assurance that progress is being made, with this matter being a standing item on the committee's agenda.

7.2 Internal audit will provide updates on the outcomes of their quarterly audits to the Quality Assurance Committee.

8.0 Action being requested

8.1 The Board is requested to **RECEIVE** and **NOTE** this report.