NHS
East London
NHS Foundation Trust

REPORT TO THE QUALITY ASSURANCE COMMITTEE
17 September 2020

Title	Data Security & Protection Toolkit – annual compliance 2019 - 20
Author	Associate Director of Information Governance / Data Protection Officer – Chris Kitchener
Accountable Executive Director	Deputy Chief Executive – Paul Calaminus

Purpose of the Report:

To advise the Quality Committee on the Trust's annual compliance with the Data Security and Protection Toolkit (DSPT) submitted to NHS Digital on 5th May 2020.

Summary of Key Issues:

Organisations are in normal circumstances required to submit their annual compliance rating by 31st March each year. Given the COVID 19 pandemic this year the submission date was extended to 30th September 2020, giving organisations an additional six months for completion.

On 31st March 2020 a number of ICT based Assertions were incomplete. This was addressed by 5th May 2020. The Trust's 2019 – 20 assessment is now complete and has been uploaded to the DSPT with a rating of 'Standards met'.

Given COVID priorities there are some areas where the evidence met the Assertion requirement but will require further work to retain compliance for 2020 – 21.

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

Implications:

Equality Analysis	Ensures every individual's personal information is handled in accordance with the law
Risk and Assurance	Provides assurance that the Trust is compliant with the Health & Social Care Act 2015, Data Protection Act 2018 & General Data Protection Regulation
Service User/Carer/Staff	The Trust has a duty to keep an individual's personal information safe. The DSPT provides a framework for effective management
Financial	There may be a need for resource to address specific areas of the DSPT
Quality	There is scope to address parts of the DSPT through quality improvement

Supporting Documents and Research material

The DSPT submission spreadsheet is in excess of 30 pages and is available from the Associate Director of Information Governance on request.

Glossary

Abbreviation	In full

DSPT	Data Security & Protection Toolkit
IGSG	Information Governance Steering Group

Committees / meetings where this item has been considered

Date	Committee / meeting
29th May 2020	Information Governance Steering Group
15th July 2020	Quality Committee

1.0 Background and history

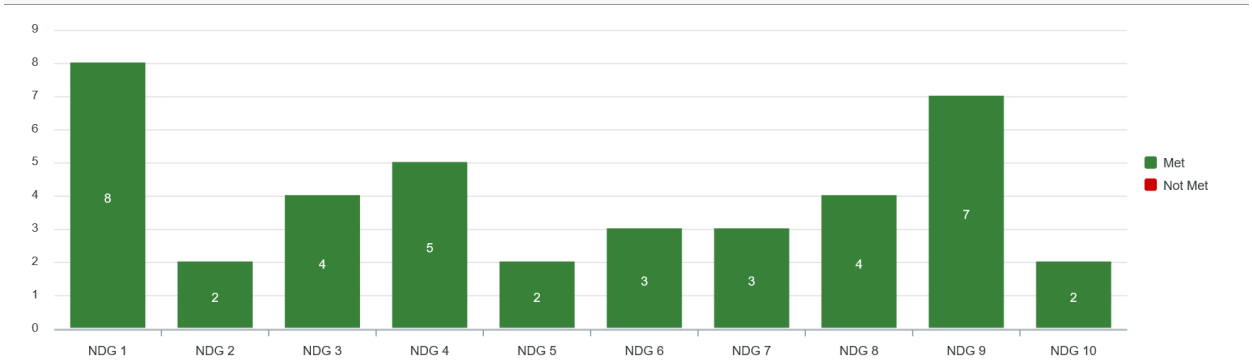
1.1 There are ten data security standards with a range of Assertions for each, 44 Assertions in total. There are 116 mandatory evidence items plus a number of non mandatory evidence items. Most organisations, ELFT included, do not currently submit evidence for non-mandatory evidence items.

1.2 The Trust submitted its 2018 - 19 assessment on 31st March 2019. At that stage it was 85% compliant (34 out of 40 Assertions completed). The assessment was published as 'Standards not fully met, plan agreed' with an action plan for compliance by 31st August 2019. Unbeknown to the Trust, NHS Digital assessed the action plan and amended our compliance to 'Standards met' on 27th January 2020. Due to an error this was not communicated to the Trust.

1.3 The assessment submission date is normally 31st March each year. This year due to the COVID 19 pandemic NHS Digital decided to extend the submission date to 30th September 2020 to provide six months grace for those Trusts who were unable to respond fully to the Toolkit requirements.

1.4 On 31st March 2020 there were a number of ICT related Assertions where evidence had not been provided. We therefore delayed our submission to 5th May 2020 by which time the ICT team had provided enough evidence to ensure compliance.

1.5 The Trust therefore submitted a 'Standards met' rating, as below.



NDG 1 - Personal Confidential Data
NDG 2 - Staff Responsibilities
NDG 3 - Training
NDG 4 - Managing Data Access
NDG 5 - Process Reviews
NDG 6 - Responding to Incidents
NDG 7 - Continuity Planning
NDG 8 - Unsupported Systems
NDG 9 - IT Protection
NDG 10 - Accountable Suppliers

1.6 Given the priorities of COVID 19 some of the evidence provided is adequate but not as robust as intended. This will therefore need to be addressed during the 2020 – 2021 submission. This is outlined below.

2.0 Annual internal audit

2.1 Organisations are required to have an independent annual internal audit. The audit is seen as supportive and helps determine what needs to be done between the audit taking place and DSPT final submission.

2.2 This year the five Assertions across two of the ten Data Security Standards were audited. The audit focussed on Managing Data Access and IT Protection.

2.3 Four recommendations were made, all low risk. All recommendations have been addressed. The internal auditors have confirmed compliance fo

3.0 Assessment of compliance

3.1 Significant improvement has been made over the past year, providing a good basis on which to build a robust evidence base.

3.2 Assertions likely to require careful management for the coming year:

Area to be addressed	Status & future requirement
National Data Opt Out policy	2019/20 compliance achieved by introducing a manual process. Requires automated process to be put in place
Records of processing activities	Identified as an issue through the ICO audit. Considerable work took place but process for maintenance / updating necessary
Information asset registers	Identified as an issue through the ICO audit. Considerable work took place but process for maintenance / updating necessary
Data security awareness training	95% compliance achieved by September 2019. Challenges in use of OLM plus classroom sessions whilst staff are working remotely or covering for colleagues to be addressed and managed
Anti-virus / anti malware protection	Top level screenshot evidence provided but requires updating & greater granularity of evidence
CareCERT alerts	Top level screenshot evidence provided but requires updating & greater granularity of evidence
Unsupported systems	Difficulties in routinely engaging with SIRO, hopefully addressed through appointment of Board level Digital Services Officer
Network configuration	Top level screenshot evidence provided but requires updating & greater granularity of evidence together with evidence of management & rationale
IT supplier due diligence	Assurance of supplier certification provided but only for specific examples & needs to be routine

3.3 This is based on an assumption that the above Assertions do not significantly change.

3.4 We are aware that Cyber Essentials requirements will be mandatory in future.

4.0 Action being requested

4.1 Quality Assurance Committee is asked to:-

a) RECEIVE and NOTE the report.