Data Security & Protection Toolkit 2020-2021 Annual Report

1.0 Background and history

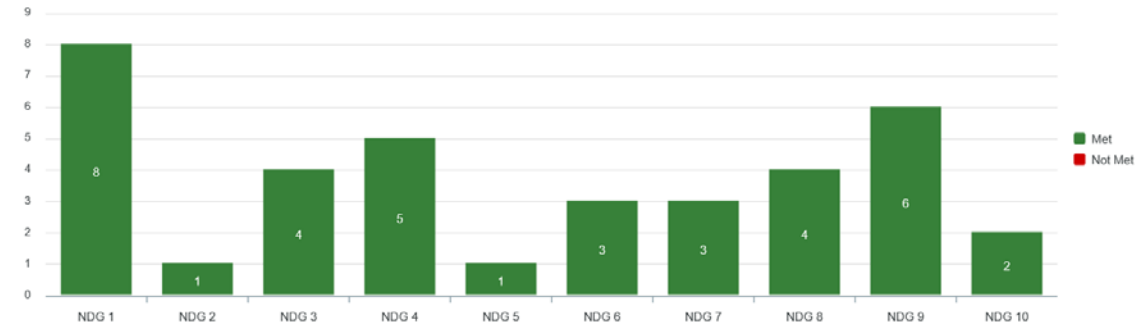
1.1 All NHS organisations are required to meet the ten National Data Guardian data security standards of the Data Security & Protection Toolkit and submit an annual assessment comprising 42 assertions made up of 110 mandatory evidence items.

1.2 There are also a number of non-mandatory evidence items. ELFT, in line with numerous other trusts, does not provide evidence for non-mandatory items.

1.3 The assessment submission date is normally 31st March each year. Due to the COVID 19 pandemic NHS Digital extended the 2019 – 20 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 This then resulted in the 2020 – 21 DSPT being unavailable until November 2020. Requirements were then published with a completion date of 30th June 2021.

1.5 The Trust submitted a 'Standards met' rating on 30th June 2021, 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 The shortened time scale affected evidence gathering and submission .Evidence is adequate but will be strengthened for the 2021 – 22 submission.

2.0 Annual internal audit

2.1 Trusts are required to have an internal audit. Ours took place in December 2020. Five assertions were selected:

Data Security Standard	Assertion
DSS 6	6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway. 6.3 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.
DSS 7	7.3 You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.
DSS 8	8.1 All software and hardware has been surveyed to understand if it is supported and up to date.
DSS 9	9.3 Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.

2.2 The auditors made recommendations in respect of 7.3, 8.1 and 9.3

Recommendation
7.3.1 The Trust will submit evidence of agreement in place with NHS Digital concerning incident response management.
7.3.5 The Trust will submit evidence of successful restore from a backup.
7.3.6 The Trust will submit evidence of the agreement with the third-party hosting backups as backups should be kept separate from the network ('offline'), or in a cloud service designed for this purpose.
8.1.3: The process of removing or updating all updated devices will be completed, and evidence of all devices being up to date will be submitted. Devices that are running out-of-date unsupported software and no longer receive security updates (patches) will be removed from the network, or the software in question will be uninstalled.
9.3.1: Evidence of patching agreements for third-party hosted applications which handle sensitive information or key operational services will be obtained and submitted.
9.3.2: The Trust will submit evidence of the SIRO review of the penetration testing results and action plan.

2.3 All evidence was subsequently provided to the auditors and the audit report made available to NHSD to satisfy DSPT 9.4.6 (what level of assurance did the independent audit of your DSPT provide to your organisation?)

2.4 New guidance also suggested NHS Digital would additionally select a number of Trusts to directly audit. We were not selected but this may be done retrospectively.

3.0 Assessment of compliance and future management

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

3.2 Evidence provision in some cases was difficult to obtain, and last minute, impacting on our ability to take a measured approach and properly scrutinise evidence. This is mostly due to the effects of Covid 19 and need to focus on the pandemic. To mitigate any risks in future we will:

- Set deadlines for submission of evidence well in advance of the national deadline
- Re-introduce an annual ad hoc IGSG where assertion owners will be required to summarise their evidence and compliance with timescales (planned in 2022 for early February provided the DSPT reverts to its standard submission timetable)

- Require assertion owners to take full responsibility for their own evidence rather than the current reliance on the information governance team to manage on their behalf

- Commission a robust internal audit at an earlier stage to provide independent scrutiny

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

Area to be addressed	Status & future requirement
Information asset registers	Currently being refreshed but given new services / ICS etc need to ensure assets and data flows are captured
Data security awareness training	95% compliance achieved but very last minute and reliant on IG team management. Challenges in both delivery and provision of accurate compliance
ICT evidence	Heavy reliance on screenshots but also need refreshed reports / procedures etc to support evidence provision in some cases
IT supplier due diligence	Assurance of supplier certification provided but only for specific examples & needs to be routine

3.4 This is based on an assumption that Assertions do not significantly change.

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