The Shrewsbury and Telford Hospital NHS Trust

Board of Directors' Meeting
11 March 2021

Agenda item	058/21			
Report	Data Security and Protection Toolkit (DSPT) Baseline Submission and associated issues.			
Executive Lead	Senior Information Risk Owner (SIRO) (Director of Governance and Communications)			
√ tick only those applicable	**Link to strategic pillar:**		**Link to CQC domain:**	
	Our patients and community		Safe	
	Our people		Effective	
	Our service delivery		Caring	
	Our partners		Responsive	
	Our governance	√	Well Led	√
√ tick / input only those applicable	**Report recommendations:**		**Link to BAF / risk:**	
	For assurance		BAF 6, 8.	
	For decision / approval		**Link to risk register:**	
	For review / discussion		ID1492, ID1676, ID1662, ID1663	
	For noting	√		
	For information			
	For consent			
Presented to:	Information Governance Committee (IGC), 9 February 2021			
Dependent upon (if applicable)**:**	-			
Executive summary:	Each year, the Trust completes and submits the DSPT. This is a performance tool produced by NHS Digital. NHS Digital expects organisations to achieve the "standards met", which defines as completion of all the assertions made, annually by 31st March. This is the usual annual date for completion. However, due to COVID-19, organisations have been informed that they have until 30 June 2021 to complete the 2020/21 submission. At the time of the IGC on 9 February 2021, 79 out of 111 "mandatory evidence" items had been completed and 21 of 42 "assertions" had been completed. Baseline information is provided for information.			
Appendices	None			

1.0 Introduction

1.1 The DSPT draws together the legal rules, central guidance and presents them in one place as a set of IG, IT and Cyber Security assertions. The toolkit allows organisations to measure their performance against the National Guardian's 10 data security standards.

1.2 The 2020/21 final submission is due for completion by 30 June 2021. However, a baseline submission was required to be submitted this year by 28 February 2021 – which indicates the extent of the progress that has so far been made against the requirements.

2.0 Baseline submission

2.1 At the time of the IGC on 9 February 2021, 79 out of 111 "mandatory evidence" items had been completed and 21 of 42 "assertions" had been fully completed.

2.2 The submission was completed and signed off by the SIRO and Caldicott Guardian.

3.0 History of compliance

3.1 The Trust has a poor (recent) history of compliance with the DSPT:

Status	Date Published
20/21 Baseline	26/02/2021
19/20 Standards Not Fully Met (Plan Agreed)	01/10/2020
19/20 Standards Not Met	30/09/2020
19/20 Baseline	31/10/2019
18/19 Standards Not Fully Met (Plan Agreed)	28/03/2019
18/19 Baseline	12/11/2018

3.2 Due to the extent of work still required to be completed before 30 June 2021, the SIRO is almost certain that the Trust will receive a "Standards not Met" status for the 2020/21 submission.

4.0 Proposed changes to the IG assurance structure

4.1 Following discussions with the Caldicott Guardian, the SIRO has proposed and agreed to chair the IGC moving forwards, which reflects usual practice. The SIRO has previous experience and success in this area.

4.2 The Caldicott Guardian will set up a separate group looking at issues relating to the security and governance of patient information and data, and will report into the IGC.

4.3 The IGC will meet on a regular basis to assess risks to security and integrity of information, and management of confidential information. The Committee will

closely monitor progress with completion of the Data Protection Security Toolkit submission, data flow mapping, information risks, and information asset registers.

4.4 The SIRO is also responsible for providing written advice to the Accounting Officer on the content of the Annual Governance Statement in regard to information risk and security.

4.5. The assurance framework partly aims to ensure that each information asset has a clearly defined administrator/manager who is responsible for that asset on a day to day basis. That manager implements the IG policies, procedures and instructions to manage that asset and provides regular reports to the Information Asset Owner (IAO) for that asset, who is responsible and accountable for ensuring that information assets within their area are managed. Currently, this is not the case. It appears that the wrong level of personnel are expected to fit into the role, and with little education / training. This is not the fault of those currently in the role, nor the fault of those attempting to provide the required knowledge to undertake the role.

4.6 But resource is required to identify the appropriate asset owners, and then to provide the training. We are also looking at the possibility of procuring an IT solution.

4.7 The organisation has in place a qualified and knowledgeable Data Protection Officer (DPO), who is responsible for overseeing the Trust's data protection strategy and its implementation to ensure compliance, as such, they must have direct access to the Board. By law, the DPO must be provided with the resources required to fulfil their role. Currently, this is not the case. A review is being undertaken of the IG team and it is envisaged that at least one more IG officer will need to be sourced to support workload – policies remain out of date, more training needs to be taken in the Trust and more IG awareness needs to be put in place - as SIRO, I even find myself signing off FOI requests on a daily basis.

5.0 Conclusion

5.1 Clearly, this governance area requires greater scrutiny, and it will take some time to get back on track. But I remain confident that compliance will be achieved with the right resources.

Anna Milanec
SIRO,
Director of Governance
March 2021