Sherwood Forest Hospitals NHS Foundation Trust

Board of Directors Meeting in Public

Subject:	2017/18 Data Security Protection Requirements	**Date:** 26th April 2018	
Prepared By:	Shirley A Higginbotham, Head of Corporate Affairs and Company Secretary		
Approved By:	Shirley A Higginbotham, Head of Corporate Affairs and Company Secretary		
Presented By:	Paul Robinson, Chief Finance Officer		
Purpose			
The Board are asked to: Consider and approve for submission the compliance with the 10 standards outlined in the 2017/18 Data Security Protection Requirements.		**Approval**	**x**
		Assurance	
		Update	
		Consider	

Strategic Objectives				
To provide outstanding care to our patients	**To support each other to do a great job**	**To inspire excellence**	**To get the most from our resources**	**To play a leading role in transforming health and care services**
✓	✓	✓	✓	✓

Overall Level of Assurance				
	Significant	**Sufficient**	**Limited**	**None**
		x		

Risks/Issues	
Financial	There are no risks or issues identified in this report
Patient Impact	
Staff Impact	
Services	
Reputational	

Committees/groups where this item has been presented before

Executive Summary

NHS Foundation trusts are required to confirm whether or not they comply with the 10 standards outlines in the 2017/18 Data Security Protection Requirements (DSPR).

The 2017/18 DSPR standards are:

1. Senior level responsibility
2. Completion of the Information Governance toolkit v14.1
3. Preparing for the introduction of the General Data Protection Regulation in May 2018
4. Training Staff
5. Acting on Care CERT advisories
6. Business continuity planning
7. Reporting incidents
8. Unsupported systems
9. On-line cyber and data security assessments
10. Checking Supplier Certification

The Trust is asked to confirm if the standards are implemented (fully, partially or not)

The Information Governance team, NHIS and the Business Continuity team have reviewed the questions and recommend fully implemented for standards 1- 7 and partially implemented for standards 8 – 10.

Public - Board of Directors

2017/18 Data Security Protection Requirements **26th April 2018**

Author – Shirley A Higginbotham, Head of Corporate Affairs and Company Secretary

Introduction

In order to improve data security and protection for health and care organisations, the Department of Health and Social Care NHS England and NHS Improvement published 10 data and cyber security standards in January 2018.

All providers of health and care must confirm whether or not they are complying with the 2017/18 Data Security Protection Requirements (DSPR) by submitting a response to NHSI before the 11th May deadline.

All submissions will be reviewed by NHS England and NHS Digital to create a baseline of cyber readiness across the sector. Initially this information will be used to target improvement support and resources and in the longer term cyber security will be considered as part of provider oversight arrangements.

Should a provider not respond they will automatically be considered as non-compliant

The questions below test how compliant the Trust is with the 10 standards, the Trust is asked to respond either fully, partially or not. Full details of the criteria is provided at appendix a

Leadership Obligation 1: People

1. **Senior Level responsibility**

There must be a named senior executive responsible for data and cyber security in the organisation

Fully Implemented

2. **Completing the Information Governance toolkit v14.1**

By 31 March 2018 organisations are required to achieve at least level 2 on the Information Governance (IG) toolkit

Fully Implemented

3. **Preparing for the introduction of the General Data Protection Regulation (GDPR) in May 2018**

The trust is asked to confirm if it has an approved plan to detail how it will achieve compliance with the GDPR

Fully Implemented

4. Training Staff

All staff must complete appropriate annual data security and protection training

Fully Implemented

Leadership Obligation 2: Process

5. Acting on Care CERT advisories

The Trust must confirm a primary point of contact to receive and co-ordinate responses to CareCERT advisories, act on CareCERT advisories where relevant and also confirm within 48 hours that plans are in place to act on High Severity CareCERT advisories, providing evidence through Care CERT Collect.

Fully implemented

6. Business continuity planning

The Trust is asked to confirm a it has a comprehensive business continuity plan to support the organisation's response to data and cyber security incidents.

Fully implemented

7. Reporting incidents

The Trust must confirm it has a process in place for staff to report data security incidents and near misses

Fully implemented

Leadership Obligation 3: Technology

8. Unsupported systems

The Trust must confirm it has identified unsupported systems and has a plan in place to remove, replace or actively mitigate or manage the risks associated with unsupported systems

Partially Implemented

9. On-site cyber and data security assessments

The Trust must confirm it has undertaken or signed up to an on-site cyber and data security assessment by NHS Digital and act on the outcome of that assessment, including any recommendations.

Partially Implemented

10. Checking Supplier Certification

The Trust should ensure that any supplier of critical IT systems which could impact on the delivery of care, or process personal identifiable data has the appropriate certification.

Partially Implemented

Appendix a

Question	Fully Implemented	Partially Met	Not Implemented
1	The organisation has a named senior executive who reports to the board who is responsible for data and cyber security and this person is also the Caldicott Guardian Name: Shirley A Higginbotham Job title: Head of Corporate Affairs & Company Secretary Name of organisation: Sherwood Forest Hospitals NHS Foundation Trust Email: shirkey.higginbotham@nhs.net Telephone number	The organisation has a named senior executive who reports to the board who is responsible for data and cyber security but this person is not the SIRO	The organisation does not have a named senior executive who is responsible for data and cyber security
2	The organisation has completed the IG toolkit, submitted its results to NHS Digital and obtained either level 2 or 3.	The organisation has completed the IG toolkit and submitted its results to NHS Digital but has not attained level 2.	The organisation has not completed the IG toolkit and submitted the results to NHS Digital
3	By May 2018, the organisation will have an approved plan to detail how it will achieve compliance with the GDPR. This will have board-level sponsorship and approval.	By May 2018, the organisation will have a plan that has been developed but not yet sponsored and	A plan has not been yet been developed.

		approved at board level on how it will achieve compliance with the GDPR.	
4	At least 95% of staff have completed either the previous IG training or the new training in the last twelve months.	The organisation has completed the IG toolkit and submitted its results to NHS Digital but has not attained level 2.	The organisation has not completed the IG toolkit and submitted the results to NHS Digital
5	The organisation has registered for CareCERT Collect		The organisation has not registered for CareCERT Collect
5	Yes - The organisation has plans in place for all CareCERT advisories up to 31/3/2018 that are applicable to the organization (**Note**: the plan could be that the board accepts the residual risk)	No - The organisation does not have plans in place for all CareCERT advisories up to 31/3/2018 that are applicable to the organisation	Not applicable - The organisation has not registered for CareCERT Collect
5	The organisation has clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT	The organisation does not have clear processes in place	The organisation does not have clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in

	advisory being issued that a plan is in place.	that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place, but is developing these processes	place, and these processes are not under development
5	The organisation has in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, but is in the process of filling that role.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, and no plans are in place to fill that role.
6	The organisation has an agreed business continuity plan(s) for cyber security incidents in place. The plan(s) take into account the potential impact of any loss of services on external organisations in the health and care system.	The organisation is developing a business continuity plan(s) for data and cyber security incidents. The plan(s) will take into account the potential impact of any loss of services on external organisations in the	The organisation does not have a continuity plan for data and cyber security incidents in place

		health and care system.	
6	Yes - The business continuity plan for cyber security incidents in has been tested in 2017/18.		No - The business continuity plan for cyber security incidents in has been tested in 2017/18.
7	The organisation has a process or working procedure in place for staff to report data security incidents and near misses	The organisation is developing a process or working procedure for staff to report data security incidents and near misses	The organisation does not have a process or working procedure in place for staff to report data security incidents and near misses
8	The organisation has reviewed all its systems and any unsupported systems have been identified and logged on the organisation's relevant risk register	The organisation has reviewed all its systems and any unsupported systems have been identified but not logged on the organisation's relevant risk register. Partially pending response from IAO's and completion of IAR's	The organisation has not reviewed its systems to identify any that are unsupported
8	By May 2018 the organisation will have developed a plan to remove, replace or actively mitigate or manage the risks		By May 2018 the organisation will not have a plan in place to remove, replace or actively mitigate or manage the risks associated with unsupported systems

	associated with unsupported systems		
9	The organisation has undergone an NHS Digital on-site cyber and data security assessment. This will be completed on April 17th	Prior to 31 March 2018 the organisation signed up to undergo an NHS Digital on-site cyber and data security assessment but has not yet	Prior to 30 March 2018 the organisation has not signed up to an NHS Digital on-site cyber and data security assessment
9	The organisation has an improvement plan in place on the basis of the findings of the assessment, and has shared the outcome with the relevant commissioner(s)	The organisation has an improvement plan in place on the basis of the findings of the assessment, but has not yet shared the outcome with the relevant commissioner(s). This will be generated from the assessment on 17th April	The organisation does not yet have an improvement plan in place on the basis of the findings of the assessment, and has not yet shared the outcome with the relevant commissioner(s)
9	Yes - The organisation has used an external vendor to audit the organisation's data and cyber security risks		No - The organisation has not used an external vendor to audit the organisation's data and cyber security risks
10	The organisation has checked that the suppliers of all its IT systems have	The organisation has checked that the	The organisation has not checked whether its suppliers of IT systems have appropriate certification.

	appropriate certification, and can evidence that all suppliers have such certification.	suppliers of IT systems that relate to patient data, involve clinical care or identifiable data have appropriate certification, and can evidence that all suppliers have such certification.	