BOARD OF DIRECTORS MEETING (Open)

Date: 9 May 2018

10

TITLE OF PAPER	**Data Security Protection Requirements – Compliance Statement**
TO BE PRESENTED BY	Phillip Easthope
ACTION REQUIRED	For approval

OUTCOME	To approve Compliance with Data Security Protection Requirement (DSPR)
TIMETABLE FOR DECISION	9 May 2018
STRATEGIC AIM **STRATEGIC OBJECTIVE** **BAF OBJECTIVE No AND TITLE**	Quality and Safety Effective Quality Assurance and Improvement will underpin all we do A101i Inability to provide high quality care due to failure to meet regulatory standards (registration and compliance)
LINKS TO OTHER KEY REPORTS / DECISIONS	Data Security & Protection Toolkit submission GDPR readiness
LINKS TO OTHER RELEVANT FRAMEWORKS, RISK, OUTCOMES ETC.	Links to revised Data & Information Governance policies, framework and strategy
IMPLICATIONS FOR SERVICE DELIVERY AND FINANCIAL IMPACT	Adherence to national standards will help protect services from disruption by cyber incidents
CONSIDERATION OF LEGAL ISSUES	GDPR will come into force in May 2018

Author of Report	John Wolstenholme
Designation	Information Manager
Date of Report	9 May 2018

SUMMARY REPORT

Report to: Board of Directors

Date: 9 May 2018

Subject: Data Security Protection Requirements Submission

From: David Hush, Head of Informatics & Information Systems

Prepared by: John Wolstenholme, Information Manager

1. Purpose

For Approval	*For a collective decision*	*To report progress*	*To seek input from*	*For information*	*Other (please state below)*
√					

2. Summary

NHS Improvement have requested Trusts to report on their progress implementing the 10 Data Security Protection Requirements for 2017/18. Submission is due by Friday 11 May 2018 and requires Board sign-off.

In January 2018, to improve data security and protection for health and care organisations the Department of Health and Social Care, NHS England and NHS Improvement published a set of 10 data and cyber security standards – the 17/18 Data Security Protection Requirements (2017/18 DSPR) – that all providers of health and care must comply with.

The 2017/18 DSPR standards are based on those recommended by Dame Fiona Caldicott, the National Data Guardian (NDG) for health and care, and confirmed by government in July 2017.

Leadership obligation 1: People

1. Senior level responsibility

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

Ideally this person will also be your senior information risk owner (SIRO), and where applicable a member of your organisation's board.

Fully implemented

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 SIRO

Please provide the contact details of the named senior executive responsible for data and cyber security if they are in place.

Name	*Phillip Easthope*
Job title	*Executive Director of Finance*
Name of organisation	*Sheffield Health and Social Care NHS Foundation Trust*
Email	*phillip.easthope@shsc.nhs.uk*
Telephone number	*0114 3050765*

Evidence: Confirmed in IG Management Framework approved by DIGB, 28 March 2018

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

The organisation has completed the IG toolkit, submitted its results to NHS Digital and obtained either level 2 or 3.

Evidence: IG Toolkit submission, approved by DIGB 28 March 2018, available at:https://www.igt.hscic.gov.uk/

3. Preparing for the introduction of the General Data Protection Regulation in May 2018

The beta version of the Data Security and Protection toolkit was released in February 2018 and will help organisations understand what actions they need to take to implement the General Data Protection Regulation (GDPR) which comes into effect in May 2018.

Fully Implemented

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.

Evidence: GDPR Status Update & GDPR Implementation Plan submitted to EDG, February 2018

4. Training staff

All staff must complete appropriate annual data security and protection training.

As per the IG toolkit, staff are defined as: all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation.

Providers must ensure staff have completed either the new IG training tool or the previous IG training tool.

Fully implemented

At least 95% of staff have completed either the previous IG training or the new training in the last twelve months.

Evidence: Projected full-year compliance rate agreed by DIGB 28 March 2018

Leadership Obligation 2: Processes

5. Acting on CareCERT Advisories

Organisations must:

- Identify a primary point of contact for your organisation to receive and co-ordinate your organisation's response to CareCERT advisories, and provide this information through CareCERT Collect
- act on CareCERT advisories where relevant to your organisation
- confirm within 48 hours that plans are in place to act on High Severity CareCERT advisories, and evidence this through CareCERT Collect

Fully implemented

The organisation has registered for CareCERT Collect

Evidence: Confirmed by Head of IT Services 24 Apr 2018; CareCERT e-mails received by IT Operations

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)

Evidence: Confirmed by Head of IT Services 24 Apr 2018

Fully implemented

The organisation has 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 place.

Evidence: Confirmed by Head of IT Services 24 Apr 2018

Fully implemented

The organisation has in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories.

Evidence: Confirmed by Head of IT Services 24 Apr 2018

6. Business Continuity Planning

Comprehensive business continuity plans must be in place to support the organisation's response to data and cyber security incidents.

Partially implemented

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 health and care system.

Evidence: The Trust has an IT Support Business Continuity Plan but not specific plans for how services deal with data and cyber security incidents – to be reviewed during 2018/19 as part of the Cyber Security Action Plan.

If there is a business continuity plan in place has it been tested in 2017/18?

No

The business continuity plan for data and cyber security incidents has not been tested in 2017/18.

Evidence: As per item 6, plans are currently in development. Once complete the plans will be tested during 2018/19.

7. Reporting Incidents

Staff across the organisation must report data security incidents and near misses, and incidents should be reported to CareCERT in line with reporting guidelines.

Incidents should be reported to CareCERT via carecert@nhsdigital.nhs.uk or 03003035222 if part of a national cyber incident response.

Fully implemented

The organisation has a process or working procedure in place for staff to report data security incidents and near misses

Evidence: Incident Management Policy and Procedure (Including Serious Incidents) available to all staff via SHSC Intranet, Electronic incident reporting system. Cyber incidents are reported to CareCERT by IT Dept.

Leadership obligation 3: Technology

8. Unsupported Systems

Your organisation must:

- identify unsupported systems (including software, hardware and applications)

- have a plan in place by April 2018 to remove, replace or actively mitigate or manage the risks associated with unsupported systems.

Fully implemented

The organisation has reviewed all its systems and any unsupported systems have been identified and logged on the organisation's relevant risk register

Evidence: Detailed in IT Risk log

For any unsupported systems identified, has the organisation developed a plan for how it will remove, replace or actively mitigate or manage the risks of unsupported systems.

Organisations are not required to submit a plan as part of this data collection process but should be prepared to submit their plan to NHS Digital if requested.

Fully implemented

By May 2018 the organisation will have developed a plan to remove, replace or actively mitigate or manage the risks associated with unsupported systems

Evidence: Mitigating actions for each system set out in ICT Portfolio

9. <u>On-site Cyber and Data Security Assessments</u>

Your organisation must:

- have undertaken or have signed up to an on-site cyber and data security assessment by NHS Digital
- act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with your commissioner.

Fully implemented

The organisation has undergone an NHS Digital on-site cyber and data security assessment

CareCERT Assure Assessment report received 28 March 2017. Penetration Test Report, 8 Feb 2017 with recommendations.

For organisations who have undergone an NHS Digital on-site cyber and data security assessment:

Partially implemented

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)

Evidence: Outcome to be shared during 2018/19. At present, no critical risks have been identified.

Please tell us if the organisation has used an external organisation to audit the organisation's data and cyber security risks. Please note there is no requirement to use an external organisation to audit data and cyber security risks.

Yes

The organisation has used an external vendor to audit the organisation's data and cyber security risks

360 Assurance completed a Cyber Security Governance audit (report dated January 2018) which offered "Significant Assurance". In addition the Data Quality Framework Follow-Up audit, the Remote Access audit and the IG Toolkit Audit, plus a 3rd party external assessment of ISO 27001 readiness all cover elements of cyber security.

10. Checking Supplier Certification

Organisation should ensure that any supplier of critical IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification (suppliers may include other health and care organisations).

Depending on the nature and criticality of the service provided, certification might include:

NHS Digital contracts for/supplies a number of IT systems and solutions in use by multiple NHS organisations. Please note that NHS Digital ensures in each of its system procurements that appropriate data security certifications are in place from its suppliers.

Not implemented

The organisation has not checked whether its suppliers of IT systems have appropriate certification.

Evidence: Confirmed by Head of IT Services 24 Apr 2018. To be included as part of service and contract review during 2018. Progress will be monitored as part of the Data Security and Protection Toolkit work programme and submissions, to be reported to DIGB.

3. Next Steps

Following Board approval of the Trust responses they will be submitted by IMST Dept.

4. Required Actions

Board is asked to support the following recommendations:

Submission of the accompanying responses for SHSC to NHS Improvement.

5. Monitoring Arrangements

Submission of this survey is due by Friday 11 May 2018.

Ongoing compliance with data security and protection standards will be monitored by the new Data Security and Protection Toolkit which replaces the previous IG Toolkit, submitted to NHS Digital and reported to the Data & Information Governance Board.

6. Contact Details

For further information, please contact:

David Hush
Head of Informatics & Information Systems
Tel: 07970763149
Email: david.hush@shsc.nhs.uk