Cambridgeshire Community Services NHS Trust

TRUST BOARD

Title:	**Implementation of data security requirements - Appendix to Finance Report**
Action:	**FOR APPROVAL AND INFORMATION**
Meeting:	**9 MAY 2018**

Purpose:

The purpose of this paper is to provide an update to the Trust Board regarding Cyber Security compliance, and seek Trust board sign off against the Data and Cyber Security compliance standards.

	Name	**Title**
Author:	James Gingell	Assistant Director ICT & Informatics
Executive sponsor:	Mark Robbins	Director of Finance and Resources

Trust Objectives

Objective	How the report supports achievement of the Trust objectives:
Provide outstanding care	Ensures availability of key ICT & Clinical Systems
Collaborate with other organisations	Not covered in this report
Be an excellent employer	Ensures staff have a safe and fit for purpose ICT solution
Be a sustainable organisation	Ensures high availability of network infrastructure

Trust risk register
None

Legal and Regulatory requirements:
None

Equality and Diversity implications:
None

Objective	How the report supports achievement of objectives:
Achieve an improvement in the percentage of service users who report that they are able to access the Trust services that they require	Improvement in range of safe and secure access to corporate and clinical systems.
Enhance our approach to involving and capturing the experience of hard to reach / seldom heard / varied community groups	Improvement in range of safe and secure access to corporate and clinical systems.
Using the national 'A Call to Action on Bullying and Aggression', internally take action to promote our Zero tolerance policy and address bullying and aggression when it occurs.	Improvement in range of safe and secure access to corporate and clinical systems.
Ensure that the Workforce Race Equality Standard is embedded and undertake proactive work around any areas of under-representation identified. In particular, we will seek innovative methods to have co-opted representation on the Trust Board from more diverse backgrounds.	Not covered in this report.

Are any of the following protected characteristics impacted by items covered in the paper? None

Age	Disability	Gender Reassignment	Marriage and Civil Partnership	Pregnancy and Maternity	Race	Religion and Belief	Sex	Sexual Orientation
☐	☐	☐	☐	☐	☐	☐	☐	☐

Background

NHS Improvement have requested assurance NHS Trusts were compliant to the recently circulated '2017/2018 Data Security and Protection Requirements', and the Trust is required to seek approval from the Trust Board that we are compliant to this guidance.

In addition NHS England have also written to all NHS Trust Chief Executives regarding the Cyber Security Threat, and provided technical guidance and a series of recommendations set out in a lessons learned document following the "WannaCry" Ransomware Cyber Attack in May 2017. The technical support includes guidance on protecting sensitive information, use of removable memory devices, appropriate use of electrical devices, protecting accounts and social media activity, and advising of the NHS Digital Data Security Centres services who provide knowledge, training and support.

2017/2018 Data Security and Protection Requirements

The 10 data security standards are identified below (details included in Appendix A attached) along with a summary of the position against the standard

1. **Senior Level Responsibility**
   The named Senior executive responsible for data and cyber security is Mark Robbins, Director of Finance, who is also the organisations SIRO (Senior Information Risk Owner). On a day-to-day basis James Gingell, Assistant Director of ICT, manages this responsibility.

2. **Completing the Information Governance Toolkit**
   From April 2018, the new Data Security and Protection Toolkit (DSP Toolkit) will replace the Information Governance Toolkit; and this new framework will provide assurance around the 10 data security standards. Submission and compliance to annual Information Governance submissions will continue as normal.

3. **Prepare for the Introduction of GDPR (General Data Protection Regulation)**
   The Trust are already full engaged with the GDPR compliance and have a project in place to achieve this.

4. **Training Staff**
   As a requirement of their employment, all staff undertake mandatory Data Security Training. Compliance levels for this training continue to meet the required 95%.

5. **Acting on CareCERT advisories**
   In order to reduce the risk of a repeat Cyber Attack, the Department of Health commissioned NHS Digital to create a Care Computer Emergency Response Team (CareCERT) to provide a centralised cyber security function. The Trust and ICT providers now receive weekly security updates via CareCERT, and update the collection portal with any impact these threats could have on the network infrastructure and technical ICT solutions used by the Trust. Since the launch of the CareCERT process, the Trust has achieved and maintains full compliance in this area receiving high levels of assurance that the infrastructure meets the necessary standards.

6. **Continuity Planning**
   All services have local Business Continuity Plans (BCP's) which are regularly reviewed to include planning for the loss of critical ICT applications and infrastructure. The Trusts Major Incident Plan is also being updated by the Resilience Lead to make specific reference to the management of a Major ICT incident.

7. **Reporting Incidents**
   The Trust continue to utilise the Risk Management system, Datix to report and review any ICT or data security incidents. These are reviewed by the Assistant Director of ICT and investigated where necessary.

8. **Unsupported Systems**
   The Trust do not have any unsupported operating systems or applications. All clinical and business applications are regularly upgraded to ensure they remain in support, and server infrastructure is also refreshed when required to maintain support. All new ICT hardware being deployed into new accommodation sites is being installed with the latest Windows 10 Operating System. The rollout of Windows 10 across the Trust will soon be scoped to ensure all technology can receive essential security updates.

9. **On Site Assessments**
   An on-site ICT Security Assessment for key ICT providers will be undertaken during 2018/2019 via NHS Digital to further identify any security weaknesses and vulnerabilities. This engagement is currently being scoped on specific CCS infrastructure and applications, and we are waiting for NHS Digital to release more dates for on site assessments.

10. **Checking Supplier Certification**
    All suppliers and contractors contracts and relationships have been reviewed and the Trust are satisfied that there are no vulnerabilities with supplier certification about Information Security.

Conclusion

The Trust remains compliant to the 10 data security standards and seeks approval from the Trust Board to sign off our compliance, which is required by 11th May 2018.