NHS
Coventry and Warwickshire
Integrated Care Board

Data Encryption Policy

Reference Number:	This will be applied to all new ICB-wide PPSs by the Governance and Corporate Affairs Team and will be retained throughout its life span.
Version:	Version 1.0
Name of responsible Committee and date approved or recommended to Integrated Care Board Board:	Audit Committee
Date approved by the Integrated Care Board (if applicable):	1 July 2022
Next Review Date:	1 April 2024
Expiry Date:	1 October 2024
Name of author and title:	Laura Collett, IT Security Lead, ICB
Name of reviewer and title:	Phil Johns, Chief Executive, ICB
Department:	Corporate Office

VERSION HISTORY

Date	Version	Changes made to previous version	Consulting and Endorsing Stakeholders, Committees / Meetings / Forums etc.

CONTENTS

1. Introduction

NHS Coventry and Warwickshire Integrated Care Board ('the ICB') must ensure it complies with the principles of the Data Protection Act (2018) for the handling of all information, particularly personal confidential data and sensitive information pertaining to patients and staff. Information must be secure and confidential at all times. Any data stored on a PC or other removable device in a non- secure area or on a portable device such as a laptop, tablet or mobile phone should be encrypted.

2. Purpose

This policy outlines how encryption will be used to secure information to ensure the ICB complies with the NHS Information Governance Policy, standards and legal requirement.

3. Definitions

3.1 Encryption

The process of converting information or data into a code, especially to prevent unauthorised access.

Encryption software must be provided by the Information Technology Department. Your own software is not accepted by the ICB and may not meet the Department of Health's specifications.

3.2 Hashing

Also called a *message digest*, is a number generated from a string of text. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

3.3 Salt

Random data that is used as an additional input to a one-way function that hashes data, a password or passphrase.

3.4 Algorithm

A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

3.5 Asset(s)

Any information system, computer or programme owned by the ICB which stores data.

4. Duties / Responsibilities

4.1 Chief Executive

Has ultimate accountability for the ICB's Encryption Policy. Operational responsibility has been delegated to the Chief Transformation Officer.

4.2 Chief Transformation Officer / SIRO

Responsible for ensuring systems and processes are in place to prevent the transfer of unencrypted person identifiable data held in electronic format across the ICB and the NHS.

Act as the Senior Information Risk Owner (SIRO) ensuring that the ICB has policy and procedures in place for protecting and monitoring of all information security aspects.

4.3 Associate Director of Information Technology (IT)

Has lead responsibility for the operational management and delivery of the IT work stream.

4.4 IT Security Lead

Responsible for ensuring the ICB and any organisation processing data on behalf of the ICB use the latest approved and secure algorithms.

4.5 IT Department

The IT Department will:

- Encrypt all laptops
- Encrypt PC desktops
- Encrypt other mobile devices issued by the ICB
- Enable Port Control on ALL laptops / PCs connected to the ICB network.

4.6 Information Asset Owners

Have overall responsibility for ensuring that information assets assigned to them are appropriately encrypted.

4.7 Information Asset Administrators

Responsible for ensuring that information assets are secured by using the appropriate encryption.

4.8 IT Security Operations Group

Responsible for ensuring the adoption of new encryption techniques and the decommissioning of obsolete encryption algorithms are actioned appropriately.

4.9 All Staff

- Are required to comply with this policy and other Information Governance and IT policies.

- Ensure external confidential emails are encrypted.

5. Process

5.1 IT Department Process

5.1.1 Minimum Information Governance (IG) Standards

The IT Department will implement the following minimum standards in line with currently applicable NHS IG data encryption algorithms and which should be used with a recommended minimum key length of 256 bits:

- AES 256
- Blowfish
- 3DES (168bit).

5.2 Data Transfer via the Internet or by Removable Media

- AES256 encryption is employed which is available when using applications such as PGP or WINZIP.
- Data transferred using these applications will be put into a Self-Decrypting Archive (SDA).
- The password (phrase) for the archive must be of an appropriate length and complexity.
- To ensure the safety of data in transit the password (phrase) should be communicated to the recipient separately (using a separate communication medium) from the encrypted data so that the intended recipient is the only one able to decrypt the data.

5.3 Windows 7 and Windows 10

The Enterprise version of Windows 7 and Windows 10 (covered by the NHS Microsoft Volume License Agreement) includes BitLocker encryption. BitLocker provides full volume encryption using AES 256.

5.4 USB Storage Devices

BitLocker is used to encrypt USB storage devices.

5.5 Apple Devices

All Apple devices are encrypted by default using AES 256.

5.6 Hashing

Windows Active Directory (used for account and access management) stores passwords as a one-way hash, salted with the username.

5.7 Transport Protocols

Secure Hypertext Transport Protocol (HTTPS) and Transport Layer Security version 1.2 (TLS 1.2) are used to encrypt data that is being transferred. Without this protection in place the data would be transferred in ‘clear text’ and would therefore be vulnerable to interception.

5.8 External Emails

Any confidential information that is to be shared externally via email must be encrypted. ICB emails can be encrypted by pressing the encrypt icon displayed on the toolbar of the email message.

6. Consultation

This policy has been developed in consultation with the IT Security Operations Group. All ICB staff have had the opportunity to comment via consultation on the Intranet.

7. Implementation

This policy will be implemented through the day-to-day management of systems and networks through the Information Technology Department.

All staff will be informed of this policy via the Staff in Brief communication and will follow the information governance principles shared during Data, Security and Protection training.

8. Training and Support

Data, Security and Protection training as identified on the ICB's Training Needs Analysis. Advice and support can be sought from the IT Service Desk or IT Security Lead.

9. Review

This policy will be reviewed 12 months after publication by the policy author.

10. Monitoring Compliance

MONITORING COMPLIANCE WITH THE DOCUMENT					
Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual / Department responsible for the monitoring**	**Frequency of monitoring activity**	**Group / Committee which will receive the findings /monitoring report**	**Group / Committee / Individual responsible for ensuring that the actions are completed**
Compliance with industry standards for strong encryption	CareCERT, NCSC and other threat intelligence sources.	IT Security Lead	Monthly	IT Security Ops Group	IT Security Ops Group/ Information Security Management Review Group

11. References

Her Majesty Stationery Office, (2018). *Data Protection Act 2018*. http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed: 25 September 2020).
European Parliament and Council of European Union (2016) Regulation (EU) 2016/679.
General Data Protection Regulations (GDPR Search results - EUR-Lex (europa.eu) (Accessed: 19 December 2022).
NHS Data Security Standards *(Data Security and Protection Toolkit)*
International Organisation for Standardisation (ISO) *ISO27001(2017) Information Security Management.* https://www.iso.org/isoiec-27001-information-security.html

12. ICB Associated Documents

- Confidentiality and Information Sharing Policy.
- Data Protection Policy.
- Email Usage Policy.
- Information Governance Policy.
- Information Security Policy.
- Removable Media Policy
- Mobile Device Policy.

13. Equality Impact Assessment Form

DOCUMENT/ PROJECT NAME: Encryption Policy			
		Yes / No	**Comments**
1.	**Does the document affect one group less or more favourably than another on the basis of: -**		
	Race	No	
	Religion or Belief	No	
	Gender reassignment	No	
	Sex	No	
	Sexual Orientation	No	
	Age	No	
	Disability (learning disabilities, physical disability, sensory impairment and mental health problems)	No	
	Marriage and civil partnership	No	
	Pregnancy and maternity	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination are there any expectations valid, legal and / or justifiable?**	No	
4.	**Is the impact of the document / guidance likely to be negative?**	No	
5.	**If so, can the impact be avoided?**	N/A	
6.	**What alternative is there to achieving the document / guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different actions?**	N/A	
8.	**Who has consultation taken place with?**	IT Security Ops Group All ICB staff via intranet consultation.	
9.	**EIA Team:** Names and designations of the 3 people who contributed to this assessment	**1. Laura Collett, IT Security Lead** **2. Kathryn Reed, Compliance and Reporting Manager** **3. Jas Sian, IT Front Office Service Manager**	
10.	**Head of Equality and Diversity**	Rano Bains	
11.	**Date of the Assessment: (dd/mm/yyyy)**	21/07/2020	

If you have identified a potential discriminatory impact on this procedural document, please refer it to the author of the policy or strategy, together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please refer to the guidance notes**. If the document affects one group less or more favourably, you MUST complete the full EIA form (i.e. if you have answered 'Yes' to any of the above).** The full EIA form can be obtained from the Equality and Diversity Department/website.

This policy, strategy, procedure or function has to go to the Head of Equality and Diversity for final sign off.

Please return a copy to the Equality and Diversity Department: rano.bains@covwarkpt.nhs.uk