NHS
Bury
Clinical Commissioning Group

Encryption Policy

Version:	2.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	Greater Manchester Shared Service - IT Department; NHS Bury CCG Information Governance Team
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	October 2021
Review date:	July 2022
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Encryption Policy CCG.GOV.018.2.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Greater Manchester Shared Service - IT Department
This document should be read in conjunction with	• Information Governance Framework • Information Governance Policy • Confidentiality and Data Protection Policy • Record Management Policy • Information Governance Incident Reporting Policy
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Development Team
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	The corporate PA office (electronic version) CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury CCG IM&T Steering Group	February 2014
1.1 = Policy once ratified	NHS Bury Clinical Commissioning Group	February 2014
1.4 = review	NHS Bury CCG Information Governance Team	October 2021
2.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	July 2021

Encryption Policy

Contents

1. Assurance

1.1. This policy defines the encryption guidelines and standards for the NHS Bury Clinical Commissioning Group.

2. Introduction

2.1. The purpose of this document is to provide guidance to all Clinical Commissioning Group (henceforth referred to as "the CCG") staff on the use of encryption to ensure CCG information and data is transmitted securely.

2.2. This policy is designed to protect the CCG as an organisation, its constituent businesses and staff by defining the use and application of encryption technology when accessing, storing and transmitting CCG corporate, personal or patient information.

2.3. All members of staff are required to comply or abide by the terms of this policy.

3. Aims and Objectives

3.1. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

4. Definition of terms

4.1. Key terms used:

4.1.1. **Encryption**

4.1.2 Encryption is the conversion of data into an encoded form that cannot be easily understood by unauthorised people. It is in a form called 'cipher text'. It is unlawful, being a breach of confidence, for anyone, without lawful authorisation to de-cipher the code. The de-encryption is carried out when the authorised personnel has the correct key or password.

4.1.3. Automated data encryption, utilising appropriate system(s) software, regulates this process to ensure that when data is transmitted between users and across networks, the mechanisms of encryption, and subsequently decryption, are performed seamlessly and invisibly, for all registered users.

4.1.4. Manual data encryption is occasionally required, and in this instance it is the responsibility of individual personnel to prepare data for transmittal or transportation, using the tools and methods provided by the organisation.

4.1.5. Encryption is a clear indicator of secrecy. However, in certain circumstances law enforcement agencies may/will require if they come across protected information, during a course of investigation.

4.1.6. **Person Identifiable Information**

4.1.7. When an individual can be identified from the data, or, from the data and other anonymised information when compared put together it is essential that this information is treated carefully.

4.1.8. A name is the most common means of identifying someone. However, where the name is combined with other information (such as an address, a place of work, or a telephone number, hospital number) this will usually be sufficient to clearly identify one individual.

4.1.9. The vast majority of data generated by the personnel of, and the systems used by the CCG can be considered sensitive, and as such should be dealt with securely.

4.1.10. **Data Security**

4.1.11. To create an effective data protection framework the Data Protection Act (DPA) 2018 and UK GDPR 2021 should be read side by side. The DPA 2018 invariably adopted the 7 principles of the UK GDPR. Personal information is subject to a statutory duty of the CCG to maintain its confidentiality, integrity and accessibility at all times. This places specific obligations on the CCG to secure individuals' personal data; The CCG is responsible for the security of personal data collected for processing. Consequently, a strict data security policy must be enforced to protect peoples data with security or organisational measures proportionate with data type being processed.

4.1.12. A critical issue as an employee, is leaving aside any considerations, arising under the DPA Act 2018 or the Human Right Act 1998, is the liability in negligence for failing to implement appropriate security control to protect the data. There are a few possible issues:

- Confidential information could be deliberately misappropriated by an insider, perhaps a rogue employee or an onsite contractor
- The information could be lost through negligence by leaving it unattended. Hardware like laptops, phones and memory sticks (if applicable) are more susceptible to this issue.
- System failure. Contact the GMSS IT Service Desk immediately to recover the lost data. The System is backed up and may be recoverable.
- Information could be misappropriated by an outsider, perhaps through a cyber-attack, or a virus.

4.1.13. The CCG uses a safe boot encryption software, which ensures that the tool to implement the encryption process is readily available and deployed.

4.2. Encryption – Key Elements

4.2.1. The physical aspect of encryption comprises several key areas. These are the elements that put the theory of data encryption into practice in the workplace. They consist of installed software solutions and processes/procedures that, when combined, provide secure mechanisms for the access and transmission of sensitive data.

4.2.2. **Safe Boot**

4.2.3. Safe Boot Encryption is a software initiative that employs whole-disk encryption, also called power-off encryption. It encrypts a machine's hard disk and modifies the Windows operating system master boot record so that the machine automatically requests a log-on name and password at start-up. Data is completely inaccessible if a machine is turned on without the proper authentication, even if a third party has access to software tools for disk interrogation.

4.2.4. The logon name can be synchronised with a user's Active Directory credentials (i.e., their network username and password), thus enabling a single sign on.

4.2.5. Device control can also be included via the central management console, which will restrict usage of USB data storage devices, prohibiting the use of any which are not on an approved list.

4.2.6. **WinZip**

4.2.7. WinZip is a Microsoft Windows based, industry standard, compression tool (software application), that is used to compress large amounts of PC data/files into more manageable file sizes, for the purposes of storage or transmittal. To use WinZip as an encryption tool, WinZip Pro version 9, or above, is required.

4.2.8. **WinZip Password Selection**

4.2.9. Selecting the correct format of password for an encrypted WinZip file/archive ensures that if the encrypted data is acquired by an unintended third party, the likelihood of it being successfully accessed in greatly minimized.

4.2.10. WinZip uses a single private password, created by the user, to encrypt and decrypt a Zip archive. Therefore, complexity and strength of the password is an integral part of creating a secure process.

4.2.11. There are two main methods, used by third parties who may try to access (attack) password encrypted data files:

- A dictionary attack
- A brute force attack.

4.2.12. Essentially, as the name implies, a dictionary attack automatically applies thousands of common words and passwords (or combinations of) in a random attempt to match the password that has been set.

4.2.13. A brute force attack automatically tries combinations of letters and numbers in upper and lower case. This means that the more characters a password consists of, the harder a brute force attack becomes.

4.2.14. For example, it is estimated that (depending upon the processing power of the machine employed), it takes 2 months to match an eight-character password using a brute force attack, and over a year to match a ten character password.

4.2.15. This is because the number of potential combinations increases exponentially with the addition of each additional character.

4.2.16. Therefore, with WinZip AES encryption, the password strength is a key aspect to the security of the encryption.

4.2.17. The following password rules provide a strong business level of encryption.

4.2.18. The WinZip password should be:

- At least 12 characters in length
- Be random, do not contain any dictionary, common words or name
- At least one upper case character
- Have at least one lower case character
- Have at least one numeric character
- Have at least one special character e.g. $,£,*,%,&,!.
- The introduction of at least one special character, in a 12-character string, makes any password extremely difficult to match.

4.2.19. Complex length passwords require good password management and decent business processes in place. Storage and communication of the password must be regulated and secure.

4.2.20. **DO NOT** send the password with the data, by writing it on a CD or similar!

4.2.21. If help is required with the creation of suitable passwords, random password generators can be found on the Internet.

4.3. USB Memory Sticks, CD ROMs & Other Removable Storage

4.3.1 Only specifically issued, encrypted, USB keys/sticks are authorised for use.

4.3.2. They are issued by the IM&T team. Existing USB keys/sticks will not be encrypted, and they will need to be swapped for the encrypted type.

4.3.3. Use of encrypted USB sticks is restricted to authorised staff only.

4.4. External Personnel (Access Procedure)

4.4.1. Following the Safe Boot installation, external personnel who may periodically need to log on to the organisation's PCs, will need to be added to a list which will allow them access to those machines.

4.4.2. If access is required by these users, the following information should be provided to IM&T by logging a call with the IT Service Desk.

- Username
- User department / team
- User contact telephone number

4.4.3. Individual external staff members, with a log on requirement, can then be added to the Safe Boot access list.

5. Duties and Responsibilities

5.1. Overall accountability for procedural documents across the CCG lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2. Overall responsibility for the Encryption Policy lies with the Head of IT or equivalent who has delegated responsibility for managing the development and implementation of operational procedures with support and guidance from service suppliers as per any prevailing contracts.

5.3. Staff will receive training regarding the policy from a number of sources: policy/strategy and procedure manuals:

- line management
- specific Training Course
- team Meetings
- CCG website

6. Main Policy

6.1. The CCG will adhere to and abide by the national code of conduct for data encryption as specified by NHS England, in letters distributed widely via key NHS teams to cascade further to all users. To summarise, all CCG data will be encrypted at rest, for example, on desktops, laptops, portable devices, such as CDs and memory sticks, and in transit.

6.2. The CCG users must not bypass, cause to bypass or use any tools or software to bypass the encryption software installed on devices by the CCG. In addition, users are strictly prohibited from downloading, installing or using their own or other encryption software.

6.3. All users who remotely access the CCG information systems and information must do so through an encrypted connection.

6.4. All wireless connections must be encrypted.

6.5. Data being transferred across the Internet or by removable media must be encrypted using NHS approved encryption. Please contact the IT Service Desk for more information on using encryption.

6.6. IT service providers must:

- use encryption software that has been approved and on the list of CESG approved products;
- apply encryption to servers, non-console administrative access and remote access (where applicable)
- apply file integrity monitoring software to alert personnel to any modification of critical systems or content files; and
- have fully documented Key Management Procedures in place that include, but not limited to, the following:

- generation of strong keys
- secure key storage and distribution
- periodic key changes and destruction of old keys;
- split knowledge and dual control;
- replacement of known or suspected compromised keys; and
- revocation of old or invalid keys.

7. Monitoring arrangements

7.1. Performance against Key Performance Indicators via risk registers and audit activities will be reviewed periodically and used by management where applicable to inform the development of future procedural activities.

7.2. This policy will be reviewed on a yearly basis, and in accordance with the following:

- legislative changes
- good practice
- significant incidents
- guidance
- case law reported
- new vulnerabilities
- changes to organisational infrastructure

8. Relevant Standards

- ISO27001:2005 International Standard for Information Security Management.
- ISO27002:2005 Code of Practice for Information Security Management
- ISO27005:2008 International Standard for Information Security Risk Management.

9. References

- ICO Guidance on Personal Information
- Data Protection Technical Guidance
- Information Security Policy
- Acceptable Use Policy