NHS
South Warwickshire
Clinical Commissioning Group

Data Encryption Policy

Contents

Version:	2.0
Ratified by:	Governing body
Date ratified:	03 April 2013
Name of originator/author:	ACS
Name of responsible committee	Clinical Quality and Governance
Date issued:	21/11/2018
Review date:	November 2021

Date	Version	Comment / Update
03/07/2018	1.1	Amendment made by Claire Jones, Corporate Governance Manager, to update year of Data Protection Act to 2018.
24/10/2018	1.1	Reviewed and approved by Clinical Quality and Governance.
21/11/2018	2.0	Approved by Governing Body

1. Introduction

It is a paramount that NHS South Warwickshire CCG has the ability to protect all Person Identifiable Data (PID)/Commercially sensitive information from unauthorised access, disclosure or loss.

The need for encryption is a mandatory requirement, in accordance with Gateway Reference 10509 (September 2008).

The deployment of encryption solutions will prevent unauthorised access to person identifiable and/or commercially sensitive information.

NHS South Warwickshire CCG will use appropriate approved software encryption packages and approved hardware devices.

2. Purpose

This document sets out NHS South Warwickshire CCG's policy for the use of encryption for organisational purposes. This policy covers all electronically stored data, held on both static and mobile devices.

This policy has been created to enable NHS South Warwickshire CCG to comply with the following requirements:

- National NHS Procurement of software
- Requirements under the Information Governance Toolkit
- ISO 27001: Information Security Management Standard
- Gateway reference 10509 (letter to Chief Executives dated September 2008)

This policy is complementary to other NHS South Warwickshire CCG Policies and should be used/read in conjunction with them.

3. Audience

This policy applies to full-time and part-time employees of NHS South Warwickshire CCG, non-executive directors, contracted third party organisations and individuals (including agency and Bank staff), students/trainees, secondees and other staff on placement with NHS South Warwickshire CCG, and staff or partner organisations with approved access (hereafter referred to as staff).

4. Responsibilities/Duties

4.1 Individual Staff Responsibilities

NHS South Warwickshire CCG Governing Body, Directors, managers and staff are responsible for establishing, maintaining and supporting Data Encryption management, in all areas of their responsibility.

They should comply with this Data Encryption Policy and ensure effective Data Encryption management mechanisms are implemented in accordance with it. Some members of staff and Committees have particular specialist functions in relation to Data Encryption as described below.

The purpose of this policy is to protect the confidential information that the organisation holds. Any breach of this policy which could lead to loss or exposure of this information may result in disciplinary and/or legal action.

4.2 Accountable Officer

The Accountable Officer has overall responsibility for NHS South Warwickshire CCG's security and confidentiality programme and ensuring that this operates effectively. She delegates operational responsibility for encryption to the Chief Transformation Officer

4.3 Director of Strategy and Engagement Chief Transformation Officer

The Chief Transformation Officer, who is NHS South Warwickshire CCG's Senior Information Risk Owner (SIRO), is responsible to NHS South Warwickshire CCG's Governing Body and Accountable Officer in relation to Data Encryption and patient confidentiality and provides regular reports to NHS South Warwickshire CCG's Governing Body in this regard. The Arden Commissioning Support Compliance Lead assists her with the performance of her duties. The SIRO has responsibility for reporting all significant risks to senior management where appropriate and ensure that they are placed on NHS South Warwickshire CCG's Risk Register.

4.4 Arden Commissioning Support Associate for Information Technology Services

The Arden Commissioning Support Associate for Information Technology Services is responsible to NHS South Warwickshire CCG's Governing Body and Accountable Officer in relation to Data Encryption and provides regular reports to NHS South Warwickshire CCG's Governing Body, via the Clinical Quality and Governance Committee in this regard. The Arden Commissioning Support Associate for Information Technology Services has a particular role in overseeing the provision of internal advice in relation to Data Encryption, especially in relation to legislation and confidentiality.

Utilising the assistance of other senior managers within NHS South Warwickshire CCG as appropriate, the Associate – Information Technology Services will oversee the work of the contracted IT service provider.

4.5 Contracted IT Service Provider

The contracted IT service provider is the designated advisor for NHS Warwickshire, and has day-to-day responsibility for the management and support of all aspects of Data Encryption. Together with the Arden Commissioning Support Compliance Lead and Compliance and Assurance Officer they are responsible for advising all staff throughout the organisation on issues relating to their Data Encryption activities. The Arden Commissioning Support Compliance Lead will contribute to investigations into adverse incidents in relation to Data Encryption.

The Arden Commissioning Support Compliance Lead will be specifically responsible for approving the business need for writable access to be given to staff for the use of NHS South Warwickshire CCG writable devices, and the monitoring of this policy.

4.6 Directors and Line Managers

Directors and Line Managers have joint responsibility for:

- Approving and signing for the use of USB encrypted memory sticks for their departments staff (using the form at Appendix A)
- Approving and signing off the user request form (Appendix A) for writable devices to allow staff writable access and forwarding these to the Arden Commissioning Support Compliance Lead for approval

- Ensuring their staff complete all statutory and mandatory training relevant to this policy through the Personal Development Review process

4.7 Staff

Each individual member of staff is responsible for guarding against the loss or unauthorised disclosure of any person identifiable data (PID) or commercially sensitive information.

NHS South Warwickshire CCG discourages staff from saving PID/commercially sensitive information to external devices. However, where it is essential for staff to save PID/commercially sensitive information, they must only do so on approved devices.

Staff must keep their username and password confidential in line with NHS South Warwickshire CCG policies. As with conventional passwords, if encryption passwords are written down they must be done so in an unrecognisable format. Passwords should not be shared.

Staff must complete all statutory and mandatory training relevant to this policy.

If there are queries in relation to encryption the Arden Commissioning Support Associate – Information Technology Services or the Arden Commissioning Support Compliance Lead can be contacted for advice.

5. Areas of Risk

The listing below identifies the risks NHS South Warwickshire CCG may be subjected to:

5.1 PCs

All NHS South Warwickshire CCG PCs are at a potential risk from theft. NHS South Warwickshire CCG's Information Security Policy states that no data should be stored on local hard drives.

5.2 USB Connected Devices

USB connected hard drives or similar devices (eg PDAs, smart phones, digital cameras, etc) have the potential to store large quantities of data and therefore will only have 'write' access if they are on an approved 'white list'. Any devices not on the white list will have 'read only' access. To apply for a device to be added to the white list, please complete the form at Appendix A (forms will not be processed unless Line Manager and Director approval has been granted).

5.3 Laptops and Tablets

Laptops and tablets are common mobile devices which hold mobile data. This form of mobile computing is increasing within NHS South Warwickshire CCG, and there is a high risk that they can be lost or stolen. A laptop or tablet that does not have any form of encryption can allow unauthorised access to the data contained on it, and, so, must be protected. Only NHS South Warwickshire CCG issued, encrypted laptops and tablets are to be used when there is a need to store person identifiable/commercially sensitive information on a laptop or tablet. This storage should only be temporary and for a specified purpose, and the data must be securely erased when it has served its purpose.

5.4 Email Attachments

All person identifiable data (PID)/commercially sensitive information sent outside of NHS South Warwickshire CCG as an email attachment must be encrypted. Ideally, this should be done using NHSmail. However, if this resource is not available to both the sender and the recipient, it is acceptable to encrypt the email attachment. To do this contact the IT Service Desk and they will arrange for the data to be encrypted for you in line with NHS Standards for encryption (256bit strength). A delivery and read receipt for the email should be requested and the associated

password (which should consist of a combination of alphanumeric and special characters) should be sent by separate means – preferably by telephone or text message. The IT Service Desk will inform you how the recipient of the email will decrypt the data.

5.5 Memory Sticks

Memory sticks are very small, portable, mass storage devices which have the potential to extract huge amounts of data from NHS South Warwickshire CCG's computer network and must therefore be regarded as a potential threat to our information security. From the date of issue of this policy, only NHS South Warwickshire CCG issued encrypted memory sticks (with Safestick or SanDisk Cruzer logos) are to be connected to NHS South Warwickshire CCG computer equipment. These devices will only be issued where there is a proven need for their use. Any other type of memory stick will have read-only access on NHS South Warwickshire CCG devices.

Person Identifiable Data (PID) or commercially sensitive corporate data should only be put on these devices in exceptional circumstances and should be securely deleted as soon as possible. Memory sticks must not be used as a permanent storage solution for this type of data. If there are locations where this type of data is needed but not accessible on the NHS South Warwickshire CCG network, the IT Service Desk should be contacted to seek an alternative solution.

To apply for an encrypted memory stick, staff should complete the form at Appendix A.

Please ensure that any non NHS South Warwickshire CCG staff who use our computer systems (eg temporary workers, contractors, etc) are made aware of this policy.

5.6 Floppy/CD/DVD Drives

'Write' access to these drives will be blocked by default. If staff need to save data to floppy discs, CDs or DVDs, they should complete the form at Appendix A.

6. Monitoring Compliance and Effectiveness

NHS South Warwickshire CCG will monitor the activity of individuals in relation to the use of person identifiable data (PID)/commercially sensitive information on all NHS South Warwickshire CCG equipment both static and mobile. The Arden Commissioning Support Compliance Lead will carry out regular audits to ensure compliance with this policy and report the outcomes of these audits to the Arden Commissioning Support Information Governance Steering Group.

Training uptake will be monitored and recorded by Learning and Development and reported to HR & OD.

NHS South Warwickshire CCG equipment will also be checked by the IT Shared Services Department as part of normal support operations.

7. Incident & Policy Breach Reporting

All NHS South Warwickshire CCG staff are required to ensure they do not act in a way that places personal identifiable data (PID)/commercially sensitive information at risk. A number of technical solutions are available to encrypt this type of information, and staff will be given training to use these where required. Where staff are regularly handling this type of information they must ensure they are aware of and comply with NHS South Warwickshire CCG policies and procedures. Where concern that local procedures are not consistent with this policy, staff must inform their line

manager. Similarly, if staff become aware of potential breaches of this policy, they must report it to their line manager and complete an incident report form.

8. Equality Impact Assessment

	An Organisation-wide Document for the Development and Management of Procedural Documents	Yes/No	Comments
1.	**Does the document affect one group less or more favourably than another on the basis of:**		
	• Race	N	
	• Ethnic origins (including gypsies and travellers)	N	
	• Nationality	N	
	• Gender	N	
	• Culture	N	
	• Religion or belief	N	
	• Sexual orientation including lesbian, gay and bisexual people	N	
	• Age	N	
2.	**Is there any evidence that some groups are affected differently?**	N	
3.	**Is there a need for external or user consultation**	N	
4.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
5.	**Is the impact of the policy/guidance likely to be negative?**	N	
6.	**If so can the impact be avoided?**	N/A	

	An Organisation-wide Document for the Development and Management of Procedural Documents	Yes/No	Comments
7.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
8.	**Can we reduce the impact by taking different action?**	N/A	

9. References

This policy complies with the following statutes, policies and procedures.

UK law and NHS Regulations:

- The Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- The Regulation of investigatory Powers Act 2000
- Terms & Conditions of Employment
- Patient Confidentiality Directives
- Caldicott Directives (NHS Executive 1998)
- Information Governance Toolkit: Requirement 313 (Version 6.0)

NHS South Warwickshire CCG Policies:

- Data Protection Policy
- Confidentiality, Security and Sharing of Personal Data Policy
- Email Usage Policy
- Freedom of Information Policy
- Information Security Policy
- Records Management Policy
- Safe Haven Policy
- Remote Working Policy

10. Appendix A - USB Device White List and Memory Stick Request Form

Port Lockdown

As you know, every Trust computer will be having its USB ports locked down.
You will no longer be able to use non-encrypted USB memory sticks or any USB device that is not on the Trust White List.
If you need a Trust encrypted USB memory stick and/or to request for your USB device(s) to be registered on the White List, please fill in this form. Your director will need to sign off your requests.

Surname ..... Forenames .....

Job Title ..... Department .....

Location ..... Contact Number.....

Requesting a Trust encrypted USB memory stick
I would like to request a memory stick Yes ☐ No ☐

Trust encrypted USB memory sticks are 2GB and cost £14.46 per stick.
Please provide a budget code.....

For our risk register, please let us know:
Will you be accessing Person Identifiable Data? Yes ☐ No ☐
Will you be accessing Sensitive Corporate Data? Yes ☐ No ☐

You will be required to sign for the stick when you receive it, agreeing that you have read and understood the relevant policy before you start using the stick.

White list request
Directors may exceptionally authorise other USB devices which will then be placed on the "White List". Please agree with your director beforehand which device, and their special justification if this is necessary for your role.

Device (Make/Model).....Purpose.....

Type of data to be accessed: Patient* ☐ Corporate* ☐ Multimedia ☐ Other ☐

Device is encrypted: Yes ☐ No ☐

Please continue overleaf if you require additional devices.

Staff declaration
I confirm that I am requesting an encrypted USB stick and/or for the white-listing of other devices.
I confirm that the details above are accurate. I confirm that I am aware that I will need to sign for the device(s) upon receipt indicating that I have read and understood the relevant policies.

Staff member signature..... Date.....

Director's declaration
I have read and approved the request for an encrypted USB stick and/or white-listing of other device(s). I am aware of my responsibilities and am assured the relevant staff member (named above) has been made aware of their responsibilities in regard to data protection and approve the request above. I confirm that departmental policies and procedures are in place to assure the confidentiality of patient and/or corporate data when these devices are being used.

*Directors will not normally authorise White List devices for the purpose of storing or transferring patient or corporate data.

Director's signature.....

Director's name (BLOCK CAPITALS).....

Please send your signed and completed form to Information Governance, Westgate House, Market Street, Warwick, CV34 4DE.

TO BE COMPLETED BY INFORMATION GOVERNANCE

Information Governance approval.....Date.....

NHS Warwickshire

11. Appendix B: Custodian Log

USB Stick S/N	Requester	Request Form Completed Y/N	Date Given	Signature	Date Returned	USB Stick Re-formatted (Custodian to Sign)