NHS Corby Clinical Commissioning Group

NHS Nene Clinical Commissioning Group

Safe Haven Procedure for the Secure Transmission of Personal Confidential Data

Policy Number: IG 09

Version:	2.1
Approved by:	Information Governance Working Group
Date approved:	May 2018
Ratified by:	Audit and Risk Committee
Date ratified:	July 2018
Name of originator/author:	Louise Chatwyn –Information Manager
Name of responsible individual:	Neil Boughton – Deputy Director of Corporate Affairs
Review date:	May 2020
Target audience:	All Staff

Version Control Sheet

Version	Date	Who	Change
1.0		GL	First version
1.1	7/12	GL	Correct 7.2.1 re digital certificates
1.2		GL	Review
1.3	July 13	M Griffiths	Reviewed for CCG Ownership
2.0	Sept 16	Louise Chatwyn	Convert to new template and updated to reflect current legislation
2.1	05/18	L Chatwyn	Revisions to reflect changes in legislation under the General Data Protection Regulations (GDPR) and Data Protection Act Incorporate Corby CCG

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

Corby and Nene CCGs are public bodies, with information processing as a fundamental part of their purpose. It is important, therefore, that the organisation has a clear and relevant Safe Haven Procedures, and that practices are implemented throughout the CCG to ensure compliance with all appropriate legislation, and standards.

Transfers of information between an organisation's departments and sites, other NHS organisations, Councils with Social Service Responsibilities (CSSR) or other third parties are commonplace and may be achieved using a variety of transfer means and formats (ie digital and hardcopy). It is a legal responsibility of an organisation to ensure that transfers of personal information for which they are responsible are secure at all stages.

The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but can also result in the organisation being fined by the Information Commissioner.

2. Purpose

This document is a statement of the approach and intentions for the CCGs to fulfil their statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

This procedure provides guidance on how to securely send personal confidential data (PCD) via the variety of media available.

This document outlines how adherence to this procedure will ensure compliance with statutory obligations

The European Union General Data Protection Regulation (GDPR) which was adopted by the European Union in 2016, came into force in all EU Member States from 25 May 2018. GDPR is supplemented by the introduction of the Data Protection Act 2018.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of the CCGs.

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	The CCG's SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Corby CCG and Nene CCG is the Chief Finance Officer
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Corby CCG is a Clinical Executive The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO role for Nene the CCGs is fulfilled by NEL CSU Email: nelcsu.dpo@nhs.net Phone: 03000 428438
Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardian of information risks and information incidents
Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for completion of the Data Security and Protection Toolkit, actions arising to ensure compliance and subsequent workplans for continuing improvement

Information Asset Owners	Information Asset Owners (IAO) will act as nominated owner of CCG information assets. Their responsibilities will include the application of this document to the assets that they 'own'
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual Data Security and Protection training • Report information Incidents appropriately

5. What is a safe haven?

A safe haven is a term recognised to explain either a secure physical location or the agreed set of administrative communication arrangements that are in place within the CCG to ensure the safe and secure transit of confidential patient or staff information. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven procedure and principles.

The CCGs recognise that as Clinical Commissioning Groups they do not have legal rights to personal confidential data for commissioning purposes and will use anonymised, pseudonymised and aggregated data for that purpose.

De-identified data should still be used within a secure environment with staff access on a need to know basis. This is reflected in the Caldicott Principles. This principle applies to the use of Personal Confidential Data (PCD) for secondary or non-direct care purposes.

5.1 Where Safe Haven procedures should be in place

Safe Haven procedures should be in place in any location where large amounts of personal information is being received, held or communicated especially where the personal information is of a sensitive nature.

All staff should adopt the Clear Desk practice and keep the workspace clear of personal confidential data and commercially sensitive data when it is unattended.

6 Process/Requirements

The following best practice points should be observed:

6.1 Fax

The use of fax is now actively discouraged. Fax machines must only be used to transfer personal information where it is absolutely necessary to do so and no other options are available.

- Identifiers should be kept to a minimum within the document

- The minimum amount of personal data necessary for the purpose should be sent
- Notify the recipient and confirm the correct fax number for use
- Numbers should not be pre programmed into the memory dial facility
- The document should be marked ‘private and confidential‘ and marked ‘for the attention of‘ a named recipient
- Take care when dialling/inputting the fax number
- Ensure that the document is removed from the machine and not left unattended
- Confirm receipt with the recipient
- Fax machines should be turned off out of hours

6.2 Post

Incoming mail should be opened away from public areas.

Outgoing mail (both internal and external) should be securely sealed and marked ‘private and confidential’ if it contains Personal Confidential Data. Further this should be sent by a secure mail method such as signed for or registered mail.

6.3 Paper documents

Where it is necessary to remove paper files from the office, ensure that this is logged for continuity.

6.4 Computers

Do not share password access to computers or systems which contain Personal Confidential Data.

Further guidance can be found in the Information Security Policy.

6.5 Email

NHSmail is automatically encrypted in transit, therefore mail between NHS.net accounts is secure.

Emails sent to; or received from any other domain is untrusted and can be open to interception and alteration. Personal email accounts must not be used as a first choice – where this is the only option the Secure Send Facility must be instigated by the CCG.[1]

The sender should always confirm the recipient email address prior to sending, a directory service is available through NHSmail.

When sending to multiple recipients using a distribution list ensure that all recipients are authorised to receive the information.

It is recommended to use “generic (or shared) mailboxes” for the transfer of personal confidential data which supports a regular business process.

[1] Process details can be located in the Email and Internet Policy

6.6 Telephone

Ensure that

- the caller or called person is identified before discussing sensitive data and disclosing the reason for the call
- the enquirer has a legitimate right to have access to the information before disclosure is made

Do not make telephone calls which require identifying details and/or sensitive data in an area which you can be overheard (for example in Reception).

SMS Text message should not be used to convey personal confidential data.

Unless you can guarantee that the message will be delivered to and received by the correct person then it is best practice not to leave a message. If necessary the recorded message should be limited to the name and telephone number of the caller.

6.7 Physical location and security

Do not allow unauthorised persons into areas where confidential information is processed.

7 Sharing information with other organisations

Since the introduction of the Health and Social Care (Safety & Quality) Act 2015, Health and Social Care bodies have two duties: to share relevant information for the direct care of an individual and to include the NHS number when doing so.
http://systems.digital.nhs.uk/nhsnumber/staff/standards

8 Sharing information with other agencies (non NHS)

When sharing personal information with other agencies for example the Police, staff must always ensure that a current and relevant Information Sharing Agreement is in place outlining the basis for sharing. This will provide the CCG with the assurance that these organisations are able to comply with the Safe Haven principles and meet legislative and other related guidance.

9 Sharing with partners to work collaboratively as part of the Local Digital Roadmap

Sharing information within the County to support the work of the Local Digital Roadmap (LDR) is agreed through the Northants Data Governance Forum.

10 Transfers of personal data to third countries etc

Section 18 of the Data Protection Act (2018) states that:

Transfers of personal data to third countries etc

(1) The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the GDPR—
(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and
(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest.

(2) The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where—
(a) the transfer is not authorised by an adequacy decision under Article 45(3) of the GDPR, and
(b) the Secretary of State considers the restriction to be necessary for important reasons of public interest.

(3) Regulations under this section—
(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;
(b) are otherwise subject to the affirmative resolution procedure.

(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay

Third countries are defined as countries or territories that are not Member States

GDPR Article 44

Any transfer of Personal Data which are undergoing or intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions guaranteed by this Regulation is not undermined.

If PCD needs to be sent in any format to third countries this must be discussed with the Information team as the levels of protection for the information may not be as comprehensive as those in the UK. Staff may also need to check with software suppliers on the location of servers.

The General Data Protection Regulation (GDPR) limits your ability to transfer personal data to third countries where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

11 Data Flow Mapping

This describes departments where there are routine information flows of personal confidential data. The requirement to map information flows is included in the Data Security and Protection Toolkit (DSP).

Information flows are reviewed annually and further guidance is provided within the Information Asset Management Procedure.

12 Business Continuity Planning

The CCG shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

In the event of a major incident or disaster, the Organisation may recall all equipment on loan to provide core services.

13 Failure to Comply

Any failure to comply and/or breaches of this document and associated policies, procedures and guidelines will be investigated thoroughly in accordance with the organisation's disciplinary policies.

All actual and potential risks to patient and staff confidentiality should be reported as information incidents including near misses to the Information Team.

14 Monitoring and Review

Unless there is major legislation or policy changes, this document will be reviewed every two years.

15 Training

Appropriate training will be provided to all Staff commensurate with their role profile as necessary.

Training is available through ESR which can be found here:
http://www.esrsupport.co.uk/access.php

16 Distribution and Implementation

A full set of policy and procedural documents to support Information Governance will be made available via the intranet where this is in place.

Staff will be made aware of procedural updates as they occur via team briefs, management communications, shared drive availability and notification via the CCG staff intranet where this is in place. Associated Legislation and Documents

To include but not limited to:

- IG01a – Framework CSU Information Governance Framework
- IG01b – Policy CSU Information Governance Policy
- IG02a – CCG Physical Assets
- IG02b – Data Assets (application provider guide)
- IG03 – CCG Information Disclosure and Sharing Policy and Procedure
- IG04 – CCG Email and Internet Policy
- IG05 – CCG Data Security and Protection Incidents Reporting Procedure
- IG06 – CSU Confidentiality & Data Protection Policy
- IG07 – CCG/CSU Data Protection Impact Assessment Procedure
- IG08a – Framework CSU Information Security Framework

- IG08b – CCG Information Security Policy
- IG10a – Framework CSU Information Quality Framework
- IG10b – CCG Records Management Policy
- IG11 – CCG Subject Access Request
- IG12 – CSU Freedom of Information Policy and Procedure

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Data Protection Act 2018
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulation (GDPR)

17 References

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Data Security and Protection Incident Reporting tool
https://www.dsptoolkit.nhs.uk/News/31

NHS Code of Confidentiality
https://www.england.nhs.uk/wp-content/uploads/2013/06/conf-policy-1.pdf

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

General Data Protection Regulation (GDPR)
https://www.eugdpr.org/