NHS

Walsall Clinical Commissioning Group

Safe Haven Policy

Safe Haven Policy
For
Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 17 September 2018
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V 4.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	17 September 2018
Date Policy is Effective From	Date of ratification
Review date:	February 2018
Expiry date:	March 2018
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff and staff working for the CCG
National Documents	- Data Protection Act 2018 - General Data Protection Regulation (GDPR - Human Rights Act 1998 - Freedom of Information 2000 - Access to Health Records Act 1990 (where not superseded by the Data Protection Act) - Computer Misuse Act - Copyright, designs and patents Act 1988 (as amended by the -Copyright Computer programs regulations 1992 - Crime and Disorder Act - Electronic Communications Act 2000 - Regulation of Investigatory Powers Act 2000 - Common Law Duty of Confidentiality
CCG linked documents	- Freedom of Information Policy - Subject Access Request Procedure - Staff code of Conduct on Confidentiality - IG Policy - IMT policy
Distribution of the document	Intranet and reception
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice;

	disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation
Kirstie Macmillan	Information Governance officer (NHSW)
BCC Information Governance team	
Sally Roberts	Director of Governance Quality & Safety
Sara Saville	Head of Corporate Governance
Serena Causer	Corporate Governance Officer

Circulated to the following for consultation

Name/Committee/Group/	Designation
SQP	
IG function leads	
Audit & Governance Committee (A&G)	

Comments received from consultation

Name/Committee/Group	Comments
SIRO	To include other electronic devices To extend the scope to include public as well as patients
IG functional lead	Confirmation of security of email domains

Version Control Summary

Significant or Substantive Changes from Previous Version
This Safe Haven Policy has been ratified by SQP for Walsall CCG. It was adapted from a policy written by Kirstie Macmillan for NHSW

Version	Date	Comments on Changes	Author
V3.1	May 2018	Reflect General Data Protection Regulation	Serena Ellis
V3.2	August 2018	Reflect Data Protection Act 2018 and General Data Protection Regulation	Serena Ellis

Contents

1.0 Introduction

The term ‘Safe Haven’ is a term recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of patient identifiable information between organisations and sites. The term was initially meant to describe the transfer of facsimile messages but should also cover the data held and used with:

1. Blackberries
2. Ipads
3. laptops
4. Answer machines
5. Photocopiers
6. Computer Screens
7. Message Books
8. Post Trays
9. Incoming Mail
10. Photographic/Video media
11. Facsimile
12. Telephone communication

2.0 Purpose

This document seeks to provide all Organisational staff who use personally identifiable data with guidance to safeguarding the integrity, confidentiality and availability of such information in a variety of circumstances.

3.0 Scope

This policy is concerned the with personal identifying information as defined by the Data Protection Act 2018, General Data Protection Regulation and the Caldicott Committee Report, December 1997.

4.0 Conversations

All employees should respect patient/public and staff confidentiality and should take into consideration the following:

1. Ensure you cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings, and when you have information discussions with colleagues about confidential information. In these situations if you do not need to identify a patient/public/staff name then don’t.
2. Consideration needs to be given to the position of an answer phone to ensure that recorded conversations cannot be overheard or otherwise inappropriately accessed.
3. When patient/publics details are being discussed staff should bear in mind that they might be overheard by other patient/publics or staff in the same room, whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patient/publics/staff rights.
4. It is not appropriate to discuss personal information in hallways, corridors, stairways, lifts or any public place where you may be overheard.

5. When speaking to a patient/public or carer on the telephone, ask the caller to confirm their identity or ring them back. If in doubt ask for confirmation in writing or fax.
6. When speaking to a staff member from another organisation confirm their identity or ring them back using the main organisation number not a direct number and then ask for the staff member or appropriate department.

5.0 Information for Secondary Use

Information that is to be transferred for purposes other than direct patient care should not identify one person (unless identifiable information is necessary). The information should be in line with pseudonymisation, where the personal information is de-identified. The NHS number should be used as the primary identifier reducing the need for any other personal data to be shared. (If a legal basis has been established to allow the CCG to use it).

Access to personally identifiable data should be restricted to authorised users for the purposes of receiving and sending identifiable data that is expected to be used for secondary purposes and for supporting de-identification of the identifiable data.

The security of the transfer of information for secondary uses must conform to NHS good practice concerning the handling of identifiable data, as predicated by ISO 27001 and 27002 and the Connecting for Health Good Practice Guidance. Adherence to relevant good practice is particularly important as the Safe Haven may be virtual in nature and Safe Haven staff may be distributed throughout an organisation.

For identifiable information to be stored for secondary use the following must apply:

1. Only authorised and registered staff should have access to the core storage of identifiable and linked data.

2. Access must be restricted to registered, authorised users.

3. Access should be at least password controlled by individual user accounts and passwords. Accounts must not be shared between users. Further information regarding password control is within the Trust's Password Management Policy.

6.0 Release of Information

Patient/public's information may be released in cases where there is a danger to patient/publics or others.

If you receive a request from the police before you release the information you must ensure that you receive a signed WA170 form. This form has to be signed off by a member of the police force who is at least one rank higher than the requester.

All police requests received on a WA170 form must be forwarded to the Information Governance Team. If you hold the records that are needed you can release the information provided the WA170 form is correctly completed. If you have any doubts about the form please contact a member of the Information Governance Support on 01922 618318.

7.0 Release of Information over the telephone

1. Confirm the name, job title, department and organisation of the person requesting the information.
2. Confirm the reason for the information request if appropriate.
3. Take a contact telephone number e.g. main switchboard number (never a direct line or mobile telephone number).
4. Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.
5. Check with your manager if you can disclose this information.
6. Provide the information only to the person who has requested it (do not leave messages either with a person or answer machine).
7. Ensure that you record your name, date and the time of the disclosure, the reason for it and who authorised it. Also record the recipient’s name, job title, organisation and telephone number.

8.0 Guidance for dealing with information by post

1. Confirm the name, department and address of the recipient.
2. Seal the information in a robust envelope.
3. Mark the envelope ‘Private and Confidential – to be opened by Addressee only.’
4. Medical Records and bulk patient data should be sent recorded delivery as a minimum requirement.
5. When necessary, ask the recipient to confirm receipt.

9.0 Guidance for dealing with sending information via facsimile

1. Fax machines should be located in secure staff areas;
2. Patient identifiable information should be sent by fax, only when absolutely necessary.
3. The fax telephone number should be verified with the recipient.
4. The responsibility for the correct despatch of all fax messages is with the sender.
5. A test fax should be sent with confirmation from the receiver to ensure that the accurate fax number is being used
6. If there is any doubt do NOT send the document by fax transmission.
7. Use a fax cover sheet or enclose a message that contains a confidentiality statement (see point 10)
8. A separate telephone call to the recipient should be made wherever possible to confirm receipt. This is particularly important when fax information is sent outside the Organisation.

9. Received faxed documents, which contain personal information, must be stored in a secure environment.
10. Confidentiality statement for fax header:
    This fax is confidential and is intended only for the person to whom it is addressed. If you have received this fax in error, please immediately notify us by telephone on the number above and return the message to us by post. If the reader of this fax is not the intended recipient, you are hereby notified that any distribution or copying of the message is strictly prohibited

10.0 Paper documents

Patient Health records, other paper records, correspondence etc should be kept in a secure fashion.

1. All sensitive records must be stored face down in public areas and not left unsupervised at any time.
2. Incoming mail should be opened away from public areas.
3. Outgoing mail should be sealed securely and marked private and confidential. (This applies to both internal and external transfer).

11.0 Disposal of Identifiable documents

1. All confidential information must be disposed of safely.
2. Paper documents can be shredded. If a shredder is used this must be a cross shredder which is a DIN security level 3. If the shredder is not at this security level then the documents must be placed in a confidential waste container for waste disposal.
3. Computer disks, processors and other devices containing confidential information must have this information deleted before disposal.

12.0 Guidance for dealing with information by email

Safe email addresses that do not need material encrypted are those ending as ***.***@NHS.Net

Please contact the Information Governance Support for advice on encryption.

1. Do not send person identifiable information (patient name etc) over email unless encrypted
2. Use the Organisation email disclaimer, this is automatically added to most emails.

3. Use minimum amounts of information in email, If individuals can be referred to by reference numbers (such as complaints or information requests) this should be the preferred option.
4. NHS.net accounts are available to staff, emails sent via NHS.net accounts are fully encrypted as long as the recipient's email account is an encrypted account.

13.0 Guidance for the storage of identifiable data

1. All personally identifiable information should be stored within a safe haven environment; behind a minimum of two levels of security
2. Manual records should be stored within lockable cabinets where practicable or lockable rooms
3. Electronic records should be accessed on a need to know basis
4. Access to electronic databases and systems must be inline with the staff member's job role. All access must be agreed in accordance with the Systems Access Request Change Form processed by the IT Department
5. All access via the use of smartcards should be inline with the Registration Authority Guidelines

14.0 Guidance on transporting information

1. Information should only be removed when absolutely necessary
2. Information should be returned as soon as possible
3. The minimum amount of information should be removed
4. Information must be transported in a non NHS identifiable sealed container
5. Information should be secure in transit; locked out of sight preferably in the vehicles boot
6. If records are used within a patient/client's home only their records should be taken into the property. Any further records should remain secure in the vehicles boot

15.0 Monitoring

The policy will be monitored through the information governance report received by Audit & Governance Committee.