Essex Partnership University
NHS Foundation Trust

SAFE HAVEN PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG50C
VERSION NUMBER:	5 .1
KEY CHANGES FROM PREVIOUS VERSIONS:	GDPR update; 3 month extension (March 21 GC)
AUTHOR:	Information Governance Team
CONSULTATION GROUPS:	Policy Steering Group, Information Governance Steering Sub-Committee Key Information Governance Leads
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	Aug 18 (GDPR)
LAST REVIEW DATE:	Aug 18
NEXT REVIEW DATE:	~~March~~ June 2021
APPROVAL BY INFORMATION GOVERNANCE & SECURITY SUB-COMMITTEE:	September 2018
RATIFICATION BY QUALITY COMMITTEE:	TBC
COPYRIGHT	

POLICY SUMMARY

These procedural guidelines will ensure that all staff are aware of the use of Trust systems in regard of patient, staff, general wider public information / data that occurs and which ensures that processes are in place to protect, highlight actual or potential confidentiality breaches in systems.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this procedure, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is
The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SAFE HAVEN PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SAFE HAVEN PROCEDURE

Assurance Statement

This procedure aims to ensure that wherever and whenever person identifiable information (patients/staff and/or the public) flows to and from the Trust, those persons responsible for transmitting and receiving it are fully aware of Safe Haven principles and procedures.

These procedure guidelines should be read in conjunction with other relevant trust policies and procedures (see 4.0).

1.0 INTRODUCTION

1.1 The need to ensure that confidential information is safeguarded is a major concern to all staff working within the NHS. The NHS has an enviable reputation for maintaining the confidentiality of personal health information, which it acquires for the purpose of clinical care, patient administration medical records management, wider management and planning, teaching and training, disciplinary proceedings and research.

1.2 Although the term "Safe Haven was originally implemented to support contract procedures it is now recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of patient identifiable/confidential information / documentation between organisations or sites using different forms of media (e.g. fax, post, e-mail, telephones, answer phones, computer systems, electronic media, manual records, books, whiteboards and notice boards).

1.3 Person identifiable / confidential information / documentation may include information on staff, patients, companies and / or the wider general public.

1.4 Sensitive (special) Personal Information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community (e.g. health or physical condition, sexual life, ethnic origin, religious beliefs, Trade union, political opinions, criminal convictions).

1.5 Business Sensitive Information is information that, if disclosed, could harm or damage the reputation or image of an organisation.

1.6 A Safe Haven is any location that is used to send and receive identifiable / confidential information in a NHS organisation securely and confidentially. Any computerised or manual document that personally identifies a person (e.g. name, address, postcode, age, gender, payroll / hospital number, bank details, voice and visual records etc.) is classed as confidential.

1.7 A Safe Haven may be either a secure physical location or the agreed set of administrative arrangements that are in place within an organisation to ensure identifiable / confidential information is communicated safely and securely.

1.8 The Trust and its employees must ensure that wherever and whenever information flows to and from the Trust, those persons responsible for transmitting and receiving it are fully aware of safe haven principles and procedures and that they adhere to them.

1.9 The following principles detail routine practice for the transfer of person identifiable (confidential) information to and from the Trust.

1.10 Patient Health Records, other paper / electronic records, correspondence and all data should always be kept in a secure fashion.

2.0 GENERAL GUIDANCE

2.1 When sending or receiving information Trust staff must be confident that they are not breaching or compromising confidentiality.

2.2 Personal identifiable information should not be given, posted, faxed, emailed or discussed with anyone other than those who specifically need it and are authorised to have access to it.

2.3 For any forms of requests (telephone, e-mail, letter, memorandum and/or face to face etc.) where there is uncertainty about the ethics of passing on information staff should seek advice from Line Managers and / or the Trust's Information Governance Leads.

2.4 Details of the Trust's Information Governance Leads can be found on the Intranet.

2.5 Staff should be aware that the use of unique identifiers, such as the NHS Number, does not negate the need to follow these procedural guidelines.

2.6 If a safe haven room / area is on the ground floor any windows should have locks on them.

3.0 SCOPE AND PURPOSE

3.1 Scope

3.1.1 This document aims to set out the practical guidance to ensure that all transfer of person identifiable / confidential information is undertaken according to the Caldicott / Data Protection Principles.

3.1.2 This procedure is designed to be disseminated to all staff to ensure that they are aware of their responsibility to comply with the NHS Safe Haven Procedure.

3.1.3 This procedure will be reviewed periodically to keep pace with future developments arising from changes in the organisation and management of the NHS, the application of the Data Protection Act 2018, the Freedom of Information Act and other legislation.

3.2 Aims & Purpose

3.2.1 To ensure that the Trust has a Safe Haven Procedure in place and that it is communicated to all staff, so they are aware of their responsibilities when handling identifiable information and act in accordance with this procedure.

3.2.2 The purpose of this procedure is to provide:

- A definition of the term safe haven
- Advise when a safe haven is required
- The necessary procedures and requirements needed to implement a safe haven
- Rules for different kinds of safe haven
- Guidance on who can have access and who you can disclose to

3.2.3 Such procedures are required to:

- Ensure that all staff who handle information are aware of their responsibility to ensure that information remains secure and confidential at all times
- Ensure that all handling of confidential information only takes place on an strict need to know basis and only as a part of his / her legitimate activity to undertake his / her job roles in the interest of patient care
- Ensure that all staff members who are authorised to handle patient information are aware of their duty to understand the Law and comply with it.
- Ensure that all written transfers should be limited to those details necessary in order for the recipient to carry out their role.

4.0 SAFE HAVEN PROCEDURES

4.1 Please refer to Appendix 1 and Appendix 2 for the “do’s and don’ts” on how to send information by the following methods;

4.1.1 ***Incoming and outgoing faxes***

4.1.1.1 Fax Machines must only be used to transfer confidential information where it is absolutely necessary.

4.1.1.2 Each site should have a formally designated safe haven fax which is published and a template is available in the Communications section on the intranet.

4.1.1.3 Example wording for a fax cover sheet:

"This document and any attachments to it are confidential and privileged and intended solely for the use of the individual or entity to whom they are addressed. They should not be disclosed, copied or distributed without the prior authorisation of the author. Use of / action taken in relation to its contents is strictly prohibited and may be unlawful. In the event of misdirection please notify sender immediately (or as soon as possible)."

4.1.1.4 Any fax machine can be made "safe haven" for sending faxes provided that they are programmed and display the correct date, time, name of department / service and produce a "confirmation of successful transmission" slip. A copy of Appendix 2 should be laminated and displayed above / adjacent to each fax machine in order to ensure everyone using the machine has access to the safe haven processes.

4.1.1.5 If the intended recipient of a fax refuses to accept the terms of safe haven processes alternative methods of sending information should be considered (e.g. post). If no alternative is appropriate the service / team manager should be advised and if it is agreed that the fax should still be sent it must be recorded that the recipient declined Safe Haven Procedures.

4.1.1.6 If you see that faxes regularly arrive addressed for a person or department unconnected with your area, tell your line manager immediately. Do not leave it – it may be critical / urgent and in these cases you should pass the fax(es) to the correct team / service manager immediately.

4.1.1.7 The responsibility for the correct despatch of all fax messages is with the sender.

4.1.2 ***Electronic information (transfer by email)***

4.1.2.1 Email transmission over networks can have serious risks. Transfer of confidential information must be avoided unless essential to the delivery of Healthcare. Where authorised email has to be used, this must follow Trust procedure, guidance and good practice.

4.1.2.2 If patients / staff have specifically consented to communication via internet mail, consent should be obtained in writing and held on the person's health / staff record. Only sending of information of a general nature is then permitted.

4.1.2.3 Microsoft Outlook – Although this is managed and protected by the Trust's networks, staff are not permitted to send confidential personal identifiable or Trust sensitive information via this method,

external to the Trust, unless email encryption is available and used or are sending NHS.net to NHs.net.

4.1.2.4 It is the responsibility of individual staff / teams to decide whether to send other types of confidential information. Staff must arrange a document password protection with recipients if they need to send confidential documents on a regular basis. The sending of information of a general nature is permitted.

4.1.2.5 If you receive a misdirected email inform the sender so that they can resend it. Delete the email from your system (including the "deleted" box).

4.1.2.6 **Contact Centre (Only)**

In order for the Contact Centre to provide an efficient service, it must be advised on a daily basis of staff movements. Emails will be sent to the Contact Centre by teams / services to update on daily sick, study, annual leave, etc. The header for these emails should contain the wording "Daily Update" the email will be sent nhs.net to nhs.net which is a secure transfer but will still only contain the required information needed for the service to continue e.g.

- Name of person (initial and surname, e.g. J Smith)
- Location (work base, e.g. Harland)
- Reason for absence using the positive return codes (e.g. for sick leave SS)
  (Example: J Smith, Harland, is absent SS – do not send emails/texts)

4.1.3 ***Incoming and outgoing post***

4.1.3.1 Always remember to mark outgoing post correctly. Include the recipient's name and correct address.

4.1.4 ***Verbal communications, phones and answer phones***

4.1.4.1 Disclosures of confidential information to anyone unknown is strictly forbidden.

4.1.4.2 When a health professional / manager makes an entry in a shared record, it is on the understanding that all those with access to the record will respect the duty of confidentiality and will not disclose any of the record content without the appropriate permission (consent).

4.1.5 ***Information storage***

4.1.5.1 Keep information secure and confidential at all times.

4.1.6 ***Shredding***

4.1.6.1 Only cross-cut shredders are allowed to be used.

5.0 SHARING INFORMATION WITH OTHER ORGANISATIONS (NON NHS)

5.1 Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving confidential information.

5.2 The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements.

- Data Protection Act 2018
- Common Law Duty of Confidence
- NHS Code of Practice: Confidentiality
- Human Rights Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- NHS Code of Practice: Information Security
- General Data Protection Regulation

This list is not exhaustive and staff will be required to implement / take regard of any new / updated legislation as it arises.

5.3 Staff sharing confidential information with other agencies should be aware that Information Sharing Protocols and agreements need to be drawn up when sharing information, please contact the Information Governance Team for further advice. (Refer to Information Sharing Procedure)

6.0 REFERENCE TO OTHER DOCUMENTATION

6.1 These procedural guidelines should be read in conjunction with:

- Sharing Information and Consent Policy / Procedure
- Data Protection and Confidentiality Policy / Procedure
- IM&T Security Policy / Procedure
- Records Management Policy / Procedures
- IT Security Policy
- Freedom of Information Policy / Procedure
- Information Governance and Security Policy / Procedure
- NHS Code of Practice: Confidentiality
- Human Rights Act 1988

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- NHS Code of Practice: Information Security
- NHS Caldicott Principles
- Access to Health Records

This list is not exhaustive and staff will be required to implement / take regard of any new / updated legislation affecting records managements as it arises.

7.0 STAFF TRAINING

7.1 All staff working for the Trust must attend a mandatory training session on Information Governance by completing the E-Learning tool. Information Governance training is an annual requirement.

8.0 COMPLIANCE

8.1 Compliance with this procedure will be monitored through the Trust's procedure compliance programme and through spot check audits carried out by the Head of Records Management and the Information Governance Manager.

8.2 Ensure any potential breaches are reported via the Head of Records Management / Information Governance Manager and appropriately recorded via the Trust's information incident reporting system (Datix).

8.3 Any incidents reported using the Trust's incident reporting process will be monitored to identify breaches to this procedure and such incidents will be investigated. Staff should be aware that failure to comply with the safe haven principles could result in disciplinary action.

END