SAFE HAVEN PROCEDURE:

Document History

Document Reference:	IG11
Version:	Revised Policy
Ratified by:	SL/SWL CCG Senior Leadership Teams
Date ratified	Draft TBC (SL CCG) Draft TBC (SWL CCG)
Name of originator/author	Information Governance Services
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Email and Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

South Lincolnshire CCG
South West Lincolnshire CCG

Version control sheet

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author/	Version
Revised Version Serving SL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SL and SWL CCG referenced IG11.	27/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre around the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook.

CONTENTS

1. Purpose

The purpose of this document is to provide staff within NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG with the procedures necessary for the transfer and storage of person-identifiable, confidential and/or sensitive information and ensure that all staff understands the need to comply with the Data Protection Act 1998 (soon to be replaced by the Information Bill currently going through the Houses of Parliament for Approval (May 2018) and the General Data Protection Regulations which come into force on 25th May 2018.

The Caldicott Principles

Principle 1:	Justify the purpose for using the information
Principle 2:	Only use identifiable information if absolutely necessary
Principle 3:	Use the minimum that is required
Principle 4:	Access should be on a strict need to know basis
Principle 5:	Everyone must understand their responsibilities
Principle 6:	Understand and comply with law
Principle 7:	The duty to share information can be as important as the duty to protect patient confidentiality (outcome of Caldicott 2 Review)

The overall aim of the document is to ensure consistent and best practice for the privacy and confidentiality of person-identifiable, confidential and/or sensitive information.

This document is based on the formal Health & Social Care Information Centre (HSCIC) Safe Haven procedure given that they are responsible for the development and approval of Accredited Safe Havens (ASH) and therefore set the default standard to follow. In addition it has been cross referenced with the guidance that can be found at (which was issued as a consequence of the number of financial fines that organisations were receiving from the Information Commissioner: (accessed 26 1 2018)
https://www.igt.hscic.gov.uk/WhatsNewDocuments/Safe%20Haven%20Briefing_June2013.pdf

2. Background

'Safe Haven' is a term recognised throughout the NHS that refers to the communication and storage of person-identifiable, confidential and/or sensitive information. It is mandatory that secure points for the receipt of confidential information transferred to the organisation are available. Access controls and registered access levels to these secure receiving points should be restricted to those needing to access the information in order to perform their role and all staff members must be made aware of their own responsibility for ensuring the protection of personal information received in to a safe haven.
The CCG has a duty of confidentiality when handling person-identifiable, confidential and/or sensitive information.

All NHS organisations require a Safe Haven Information procedure in order to maintain the privacy and confidentiality of person-identifiable, confidential and/or sensitive information.

Historically Safe Haven processes have been associated with the use of Fax but have been extended to cover post/courier, personal conversations, telephone, fax, email, SMS messaging, Instant Messaging (IM), Web Interfaces and Portable Data Storage Devices. **The use of Fax is now actively discouraged (except where there is no other option available).**

3. Scope

The Safe Haven concept should be used to ensure good practice for all personal identifiable, confidential and/or sensitive information received and sent from the CCG and contractors should seek assurances from system suppliers concerning the security of digital communications channels.

This document provides:

- A definition of Safe Haven, person identifiable, confidential and sensitive information
- Essential requirements for the management of person-identifiable, confidential and/or sensitive information
- Guidance as to when to use the principles set out in this document
- Rules around access and disclosure of person-identifiable, confidential and/or sensitive information
- Legislation and guidance which dictates the need for a Safe Haven Procedure Rules around the different types of Safe Haven routes

The procedure applies to all permanent, temporary staff and secondees of the CCG.

The procedure applies to all person-identifiable, confidential and/or sensitive information (including business information) that may be transferred via the following formats:

- Post/courier
- Personal Conversations
- Telephone
- Fax
- Email
- SMS Messaging
- Instant Messaging (IM)
- Web Interfaces
- Portable Data Storage Devices

All routine transfers/flows of person-identifiable, confidential and sensitive information should be subject to a risk assessment and procedures should be in place to ensure receipt at a secure and protected point.

The principles and procedure in this document should be adhered to for all person identifiable, confidential and/or sensitive information processed by the CCG.

4. Responsibilities

The Senior Information Risk Owner (SIRO) is ultimately accountable for the safe use including transfer of patient related data but each member of staff has also got a duty of confidence to maintain confidentiality.

Information Asset Owners (IAO) are responsible for ensuring that information is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards apply.

Information Asset Administrators (IAA) are responsible for supporting the IAO to fulfil their responsibilities. IAAs will ensure that policies and procedures are followed, recognize actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Further guidance is available from IG Services via lynne.wray1@nhs.net or jemptage@nhs.net

5. Safe Haven Storage Requirements

Confidential, person confidential and sensitive documents and records will be stored in locked drawers or cabinets, in a locked office area with a swipe card door entry security system, limited to staff working for the CCG.

A nominated person will be responsible for the security of locked cabinets where confidential, person confidential and sensitive are stored within individual business teams. They will be responsible for the safe-keeping of the information stored in the cabinets.

Unauthorised people will not be allowed access to areas where confidential information is kept unless supervised. ID badges will be checked before access is permitted.

Business Teams that have a Safe Haven storage facility within their own work areas should ensure an appropriate tracking system is in place for all information stored in the facility.

All business areas that have person identifiable, confidential and/or sensitive information must have an appropriate Safe Haven and ensure that it meets appropriate standards.

Identification and/or approval will be required from a relevant Information Asset Owner (IAO) before a member of the CCG staff will be given access to information stored in a Safe Haven.

The person removing the information is then responsible for maintaining its confidentiality and returning it as quickly as possible to its storage place.

6. Communicating Person Confidential and/or Sensitive Information

External requesting parties should comply with the CCG Safe Haven Procedure and meet appropriate legislation and related guidance. It is the responsibility of CCG staff to ensure the receiving party is compliant before transferring the information e.g. this may be done by sending/emailing a copy of our Safe Haven Procedure to the requesting party and asking them to ensure compliance.

7. Communicating by Fax

- Given the number of incidents relating to the use of Fax that have been reported to the Information Commissioner (and where fines have been issued) the use of Fax is actively discouraged.

- Person identifiable, confidential and/or sensitive information should only be sent by fax in exceptional circumstances where other transfer methods are deemed unavailable.

- Fax machines must be kept in a secure location i.e. in a locked room out of any public area to avoid unauthorised access.

- Never send a fax to an unsupervised fax machine, unless it is a designated ‘safe haven’ or ‘secure’ machine and ensure that an appropriate person is available to receive the fax.

- Do not send large amounts of information containing person identifiable, confidential and/or sensitive information by fax.

- Do not send faxes to a destination where they won’t be seen for some time (either unattended or outside office opening hours).

- Use an alternative method to send person identifiable, confidential and/or sensitive information if the recipient does not have a fax machine in a secure environment.

- Make a telephone call to the recipient to inform them that a fax containing person identifiable, confidential and/or sensitive information is being sent, and request confirmation of receipt of the fax.

- Double check the fax number before sending and request a report sheet to confirm the transmission was successful.

- A cover sheet should be sent with the fax, which contains a confidentiality disclaimer to the effect of ‘This fax is confidential and is intended for the person whom it is addressed.’ Ensure that fax machines are switched off outside office hours.

8. Communicating by Mail

- When sending person identifiable confidential and/or sensitive information mark the envelope ‘Private & Confidential – To be opened by Addressee Only’. Confirm the name, department and address of the recipient and ask the recipient to acknowledge receipt of the information.

- Seal the information in a robust envelope using strong wrapping tape.

- Where appropriate place the document/record in double bags and send the information by Special Delivery or by courier.

- Deliver confidential incoming post immediately or as soon as possible to the recipient but do not leave on the desk or pass to anyone else if the recipient is not available. Lock in a drawer or cabinet until the recipient is available.

- Open incoming mail away from public areas. Mail must be opened by the addressee only if marked as such.

- Pass items not marked with a name or department, that are not labelled ‘Private and Confidential’ to a member of the Office Services team to establish to whom it belongs.

- Avoid sending large amounts of information about one person or information about many persons by mail.

9. Communicating by Telephone

Person identifiable, confidential and/or sensitive information should not be divulged over the telephone because of the risks involved (e.g. being overheard, inadvertent disclosure of confidential information, disclosing confidential information in an appropriate manner etc.)
If the use of a telephone is essential to convey the information then the following security protocols must be adhered to:

- Confirm the name, job title, department and organisation of the person requesting the information, ensuring that you are speaking to the correct person
- Take a contact telephone number e.g. main switchboard number *(never a direct line or mobile telephone number if possible)*
- Ring back to confirm that person's identity
- Confirm the reason for the request
- Ensure that the enquirer has a legitimate right to have access to the information before information is given out and provide information only to the person who has requested it

10. Communicating by Email

- Always consider first if email is the best way to send the information. NHS.net email is automatically encrypted in transit, therefore any email sent from one NHS.net email account to another (e.g. xxx@nhs.net to yyy@nhs.net) is secure.
- The user sending the email must first confirm the recipients correct email address, for example verbally over the telephone or through the NHS.net mail directory.
- NHS.net email is hosted on the N3 network and as such forms part of the wider public sector Government Secure Intranet (GSi). This means that email is encrypted when delivered to any of the following email domains:

Central Government
xGSI (*.x.gsi.gov.uk)
GSI (*.gsi.gov.uk)
GSE (*.gse.gov.uk)
GSX (*.gsx.gov.uk)
CJX (*.police.uk

*.pnn.police.uk *.cjsm.net)
SCN (*.scn.gov.uk)

Local Government
GCSX (*.gcsx.gov.uk)

- All emails sent between these domains are encrypted in transit and the entire environment/infrastructure is accredited with strict end point access controls.

- Emails sent to or received from any other domain is untrusted (open to forging, interception or alteration).

- When sending outside the GSi network, personal, sensitive and confidential information must be removed from the email and sent as an encrypted attachment.

- Emails containing confidential information should be clearly marked 'Confidential' in the subject header box.
- Always check that the email address(es) of the recipient(s) appear correctly in the To and Cc boxes. Automatic recognition of names can sometimes cause a problem.

- If sending to multiple recipients use a distribution list ensuring security permissions and access controls have been checked. The members of the distribution list can be checked through the Properties button when you select it.

- Always ensure that the distribution lists contains only those individuals who are authorised to receive the information.

- Do not send or forward person identifiable, confidential and/or sensitive information by email

- to any person or organisation that is not specifically authorised to receive and view that information.

- Do not send emails containing person identifiable, confidential and/or sensitive information to your home computer or personal email accounts.

- Emails containing person identifiable, confidential and/or sensitive information must be

- stored appropriately upon receipt e.g. incorporated within HR personal records and deleted from the email system when no longer required.

- SMS Text Messages should **not** be used to convey person identifiable, confidential and/or sensitive information.

11. Information Mapping

To support Save Haven principles and implementation the CCG must ensure that all information transfers are identified by determining where, why, how and with whom it exchanges information.

This is known as Information Flow Mapping. This mapping of information, particularly Personal Confidential Data (PCD will help identify the higher risk areas of information transfers that require effective management.

12. Equality Impact Assessment

The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCG legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief.

The Equality Impact Assessment has been completed and has identified impact or potential impact as “no impact”

13. Policy Review

This policy will be reviewed in line with Information Governance Toolkit requirements or where changes occur with legislation or national policy.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

SAFE HAVEN PROCEDURE

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

Name(s) and role(s) of staff completing this assessment:

June Emptage – Information Governance Officer

Date of assessment: 27 February 2018

proposed change:

Will it affect employees, customers, and/or the public? Please

state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.