GUIDELINES FOR SAFE HAVENS AND TRANSFERRING PERSONALLY IDENTIFIABLE INFORMATION (PII) & SPECIAL CATEGORY DATA

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IGSoc - GDPR Policies\IG-13 - Guidelines for Safe Havens & Transferring Personally Identifiable Information PII Special Category Data V5.0.docx

Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V4.0	April 2021	S Owen	Reviewed, minor changes
V4.1	April 2022	S Barnes	Reviewed, no changes
V5.0	Sept 2023	J Carey	Merged IG14 and IG13 Policies

Approval

Version	Name	Position	Signature	Approved Date
V3.0	IGSG	IG Steering Group		14 Mar 2018
V3.1	Badger Executive	Executive		25 July 2019

Glossary

Term	Description
PII & SCD	Patient Information Data
IGSG	Information Governance Steering Group
PII	Personally Identifiable Information
GDPR	
SCD	Special Category Data (as defined by ICO and GDPR)

1 INTRODUCTION

As a data collector and information user, Badger is responsible for ensuring that information and data is handled with care and respect. It is the responsibility of all members of staff to protect information and data from those who are not authorised to use it or view it. The organisation must ensure that everything possible is done to protect information and data and comply with the Caldicott Principles and Data Protection requirements.
Clinical environments should operate in accordance with safe haven principles.

This procedure must be adopted by anybody employed or working on behalf of Badger or who is, or may be, involved either directly or indirectly with the transfer of personal and confidential information, and special category datato contacts within and outside Badger.

1.1 Purpose of the Document

To establish clear guidelines on the safe and secure transfer of sensitive or Personally Identifiable Information and Special Category Data (PII & SCD).

Applicability This policy applies to all Badger employees who transfer sensitive PII & SCD information to external bodies, including those who send activity reports, complaints, incident investigations, commercially or financially sensitive information.

2 ROLES AND RESPONSIBILITIES

All staff in the organisation are responsible for safe receipt, maintenance, and disclosure of personally identifiable information in line with this policy and good practice.

Caldicott Guardian, SIRO, and Directors/Senior Managers have specific responsibilities to ensure compliance.

Caldicott Guardian is responsible for ensuring person identifiable information is received, stored and used in line with the Trust obligations to the Data Protection Act 2018 and the NHS Information Authority Information Governance Toolkit.

SIRO (Senior Information Risk Owner) is responsible for protecting data and managing information risks.

Directors and Senior Managers are responsible for ensuring procedures are known and followed in their areas.

All Badger staff who process person identifiable information are responsible for ensuring guidance is adhered to.

Confidentiality breaches should be reported immediately to the line manager and a serious incident form must be completed.

3 DEFINITIONS

3.1 Safe Haven:

A secure physical location or an agreed set of administrative arrangements within the organisation to ensure safe communication of confidential personal information. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means.

3.2 Personally Identifiable Information (PII):

Personal information is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different

information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

3.3 Special Category Data (SCD):

The Information Commissioners Office (ICO) has published updated GDPR guidance regarding special category data.

The GDPR singles out some types of personal data as likely to be more sensitive and gives them extra protection. Special category data relates to personal data that:

- reveals **racial or ethnic origin**;
- reveals **political opinions**;
- reveals **religious or philosophical beliefs**;
- reveals **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning an individual's **health**;
- data concerning a person's **sex life**; or
- their **sexual orientation**.

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

3.4 Business Sensitive information:

This is information that poses a risk to the company if discovered by any individual or organisation outside of the Business. This includes but is not limited to financial data, supplier and customer information. Disclosure of business sensitive information could, if disclosed, also harm or damage the reputation or image of an organisation.

4 GUIDING PRINCIPLES

4.1 Eight Caldicott Principles

The Caldicott principles are a number of recommendations aimed at improving the way the NHS handles and protects patient information:

1. Justify the purpose(s) of using confidential information
2. Use confidential information **only** when it is necessary
3. Use the minimum necessary confidential information
4. Access to confidential information should be on a strict need-to-know basis
5. Everyone with access to confidential information should be aware of their responsibilities
6. Comply with the law
7. The duty to share information for individual care can be as important as the duty to protect patient confidentiality
8. Inform patients and service users about how their information is used

4.2 Data Protection Act 2018 Principles

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (UK GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes

- Used in a way that is adequate, relevant and limited only to what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

5 REQUIREMENTS FOR SAFE HAVENS

Locations and security arrangements for safe havens should adhere to specific guidelines, including:

- A lockable room/area accessible only by authorized staff
- Ground floor windows with locks
- Compliance with health and safety requirements
- Storage of manual paper records in locked cabinets
- Computers not left on view or accessible to unauthorized staff, with secure screen saver functions and turned off when not in use
- Equipment like fax machines with a code password and turned off outside office hours (if possible).

6 PRECAUTIONS FOR HANDLING A REQUEST

All staff should be alert to the need to protect confidential information should it come their way. For the purposes of this procedure, Badger considers all its buildings with physical security access (restricted to authorised personnel) as safe havens.

When handling requests involving special category data (SCD) or personally identifiable information (PII), the following precautions must be taken:

- Seek authorisation from the Caldicott Guardian, Information Governance Lead, or SIRO if not delegated.
- Whenever possible, anonymise the data by removing any PII or SCD content

6.1 Email

Person-identifiable information and special category data must only be sent by e-mail when deemed to be absolutely necessary. This information should be sent to and from an NHS.net account. If this is not possible the identifiable information must be included within an attached encrypted password protected document, spreadsheet or database. Inclusion within the main body of the e-mail is not permitted.

- All attachments containing confidential / special category data must be password protected. The password must be delivered to the intended recipient via the telephone, or in a separate email if necessary.

- Steps must be taken to ensure that any confidential / sensitive information is sent to the mailbox of the person or persons who are authorised to see that information and that no unauthorised persons have access to said mailbox

- Before sending / receiving confidential / sensitive emails, confirm the email address with the other party, spelling any words that may cause errors. In addition, test messages must be sent.

- Use must be made of the e-mail “Tracking Options” where available to notify that a message has been delivered and / or read. Otherwise, the sender must be telephoned to confirm receipt.

- A copy of the e-mail and its attached documents must be stored appropriately within manual and / or electronic records, and the original email deleted from both the inbox and deleted items.

	Information containing PII & SCD	Sensitive Information
From nhs.net mail To nhs.net mail	Best practice, as it's a secure transfer.	Best practice, as it's a secure transfer.
From nhs.net/nhs.uk mail To any verified email account (other than nhs.net)	Data needs encrypting using 7-Zip (2) with password protection.	Authorised process; a risk assessment of sensitivity of data versus choice of appropriate email channel needs to be carried out.
From nhs.net/nhs.uk mail To hotmail, Google accounts etc…	Must not happen	Must not happen

1. Generic nhs.net email accounts are available (please ask Badger IT department) and can be created on request after being assessed by the IT department,
2. 7- Zip:
   a. Needs to be installed:
      i. on the workstation of the user sending information (contact Badger IT department).
      ii. on the workstation of the recipient from the other organisation who will be receiving the information. (**www.7-zip.org**)
   b. The user will need to familiarise themselves with brief instructions available from Badger IT department.
   c. Avoid transmitting passwords via email, use telephone if possible. If necessary, send passwords separately from the email containing PII or SCD information.

6.2 Fax

Fax machines should not be used to share personally identifiable or special category data under any circumstances, this was effective from April 1st 2020.

6.3 Verbal communication / phone

Incoming and outgoing calls may generate confidential / sensitive conversations. Caution must be exercised to ensure sensitive conversations are not overheard.

- When disclosing confidential or sensitive information over the phone consideration must be given to authenticating the caller.
  - Verify the identity and authority of individuals requesting information.
  - Record the name, date, time, reason for disclosure, and the authorising individual's details.
  - Provide information only to the authorised person. Do not leave messages.
  - Team leaders must create an entry in the shift report with all relevant details and inform the Caldicott Guardian

- If the information being given to you by the caller is confidential but irrelevant, the caller must be stopped.
- Confidential information received over the telephone must be processed appropriately, in accordance with existing standards and / or legislation.
- If information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual and in the case of an organisation obtaining the switchboard number by an independent search and then calling the recipient back.
- Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other staff who do not have a "need to know". Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.

- Messages containing personally identifiable information or special category data should not be left on answer machines unless a password is required to access them. They should also not be stored on communal systems.
- Messages containing confidential / sensitive information should not be written on whiteboards / notice boards.

6.4 Post

Where personal and confidential information must be sent by post, it should be limited to those details necessary in order for the recipient to carry out their role. The following process should be followed:

- ✓ Confirm recipient details and address.
- ✓ Seal information in a robust envelope marked "Private & Confidential to be opened by Addressee Only."
- ✓ Use tracked post for sensitive information when appropriate.
- ✓ Request confirmation of receipt when necessary.

The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

If an organisation has a policy that all mail is to be opened at a central point this policy must be made clear to all partners. An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.

6.5 Courier

- Transfer of PII or SCD information via courier must be done through secure couriers with sealed containers and tracking capabilities.
- Use courier services that provide adequate security assurances under a written contract.

6.6 Internet use

- Confidential information or data must not be transmitted over the Internet unless encrypted.
- Avoid posting confidential information on the Badger website due to the lack of encryption capabilities.

6.7 Portable storage device

- Authorised portable storage devices for transferring PII or SCD information are CDs/DVDs with encrypted files or encrypted USB keys. Contact the IT department for assistance.
- Refer to policy IG-39 - Removable Media and Acceptable Use Policy for further details.

7 MONITORING AND REVIEW OF THIS POLICY

The Information Governance Steering Group will monitor the implementation of this Policy and subsequent revisions.

The Policy will be subject to review when any of the following occur:

- The adoption of the standards highlights errors and omissions in its content
- Where other standards / guidance issued by Badger conflict with the information contained
- Where good practice evolves to the extent that revision would bring about improvement
- Analysis of incident logs show an unacceptable number or proportion are related to safe havens or transfer or PII/SCD
- 2 years elapse after approval of the current version

8 APPENDIX 1 – NHSMAIL SHARING SCD AND PII BY EMAIL

Badger will comply with the latest published guidelines from NHS Digital:

https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email