University Hospitals of Derby and Burton NHS Foundation Trust

Protecting patient confidentiality on telephone calls - Standard Operating Procedure

Reference Number: SOP-NONCLIN/ 4368/24	**Version: 2**		**Status: Draft**	**Author: Deputy Head of Information Governance (IG)**
Version / Amendment History	Version	Date	Author	**Reason**
	1	November 2022	Deputy Head of IG	**Written to set out what steps staff must follow when contacting patients via telephone**
	2	May 2023	Head of IG	**Revised version following consultation**
Intended Recipients: All UHDB staff making or taking telephone calls, particularly those in the Patient Access Centre, Waiting List Teams and all other patient administration areas.				
Training and Dissemination: To be published on IG intranet page and circulated by Head of Patient Access and Administration.				
To be read in conjunction with: Information Governance Policy, Data Protection & Confidentiality Policy/Procedure				
In consultation with and Date: • **Waiting List Team (Oct-Dec 2022)** • **Information Governance Steering Group (Jan and Mar 2023)** • **Head of Safeguarding (Feb-Mar 2023)** • **Emergency Department and Voice Services (April 2023)** • **Patient Access Group (May 2023)** • **Vulnerable Persons Group (June 2023)**				
EIRA – no EDI issues identified				
Approving Body and Date Approved	**IGSG**			
Date of Issue	**June 2023**			
Review Date and Frequency	**Every 3 years**			
Contact for Review	**Head of Information Governance**			
Executive Lead Signature	**Executive Medical Director**			

Contents

1. Background

NHS England (NHSE) encourage the use of telephone communications with patients and service users to support the delivery of care. When making or receiving telephone calls, for example, to set up an appointment, you need to follow simple safety precautions to ensure the privacy of the person you are calling. The Trust follows NHSE guidance on protecting confidentiality and privacy on the telephone.

Trust Staff are bound by the legal and ethical duty of confidentiality.

Data Protection Principles and Caldicott Principles must be applied when processing personal data. Principles relevant to this SOP are:

- 1st Data Protection Principle 'Used fairly, lawfully and transparently'.
- 1st Caldicott Principle 'Justify the purpose – there should be no 'surprises'.

The consequences of not meeting these principles include:

- Breaching of patient confidentiality which could result in relationship breakdown between clinician and patient.
- Enforcement action from the Information Commissioner's Office (regulator of data protection laws).
- Compensation claims from patients

2. Steps to follow when telephoning a patient

2.1 Before making the call:

- Double check the number before dialling.
- Check your location: make sure that your telephone conversation cannot be overheard, and that the person you are calling cannot overhear other confidential matters in the background.
- Ensure you are up to date with mandatory Safeguarding and Information Governance training. Bear in mind any Safeguarding alerts on patient systems. If any aspect of a call raises concerns do not release any information, end the call, and seek advice.
- Ask the person who answers the phone if they are ok to talk.

2.2 When calling from a landline number:

- When your call is answered: give your full name and the name of the hospital. Do not reveal the service/area you are calling from. Ask to speak to the relevant person by their full name.

- When the relevant person answers or comes to the phone: check their identity by asking for three details such as their date of birth, postcode, and the first line of their address. Once you are satisfied you are speaking to the right person, tell them the service you are calling from and the purpose of the call.

- When someone else answers the phone: give your full name and the name of the hospital, but not the service or purpose of the call. Ask if there is a better time to speak with the person and end the call, even if the recipient applies pressure to extend it. Try calling again at the suggested time if possible. Set a limit on the number of attempts made to call at different days and times and record them, before you consider sending a letter.

- If the call goes to voicemail, leave your name, the organisation/hospital where you work and switchboard telephone number. No other information should be left.

2.3 When calling a mobile number:

- Do not assume that mobile devices are more secure than landline telephones.

- Verify the person's identity before offering any details about the service you are calling from or purpose of the call.

- Check if you have called at an appropriate time and consider adjusting your questioning style to maintain privacy. For example, you do not want to be asking a person for their date of birth and first line of address/postcode if they are on public transport or in a public area.

- If the call goes to voicemail, leave your name, the organisation/hospital where you work and switchboard telephone number. No other information should be left.

2.4 If the person you are calling asks for proof of your identity:

Advise them to hang up, call the Trust's switchboard, and ask to be put through to your extension number or if working from home, ask the department to confirm validity of your call. You can then perform the simple identity verification checks described above.

IMPORTANT: Please ensure your contact details i.e., department/area, telephone extension/mobile phone numbers are up to date within the appropriate telephone directories.

2.5 If the person uses call screening:

Before you speak to the person it is acceptable to announce the hospital's name. Staff do not have to give their name for call screening, although this should be given when you start a conversation with whoever picks up the call.

2.6 If you have been unable to reach the patient after numerous attempts:

If possible, access another Trust patient system (or the NHS Spine Portal) to check that the telephone number is correct.

Under no circumstances should a patient's Next of Kin be contacted if you have been unable to contact the patient. A patient's Next of Kin is an emergency contact and must never be used as an alternative contact.

In urgent circumstances, for example, a patient's operation has been cancelled for the following day, and direct means of contact with the patient have failed, advice should be sought from the IG Team or the Caldicott Guardian to agree what action should be taken.

2.7 If during a telephone call, a patient requests email communication for future correspondence rather than post:

The Trust's email disclaimer, which can be found by clicking here and can be accessed under the section Files, must be read over the telephone. If the patient is willing to accept the risks, email communication can proceed.

When writing down an email address, take time to ensure that it has been noted correctly, for example, avoiding misspellings of names such as Clare/Claire, ensuring any numbers in the address are accurate, and that the correct domain name (such as Gmail, Yahoo!, Outlook etc.) are used.

If the department has a generic email address, the email should be sent from this account rather than a staff member's personal email account.

Before sending the email, the following steps must be followed:

- Send a test email to ensure the address is correct before sending any of the patient's personal data.
- Type **[secure]** in the subject field. It is important that it is spelt correctly and is in square, rather than rounded, brackets. NHSmail Egress is a secure service which enables the safe exchange of sensitive and patient identifiable information between different types of email account when using **[secure]**.
- Do not include any Personal Data in the subject field.
- Refer to the telephone conversation in the body of the email.
- Attach the letter as an enclosure. You may wish to password protect the document if it is of a highly sensitive nature. The password must be sent via a separate guise and not sent in an email following the initial email, in case the recipient's details are incorrect. Either text or contact the patient with the password.
- Before pressing 'Send' double check the body of the email for accuracy and ensure the correct letter is attached.

3. Steps to follow when receiving a telephone call about a patient

- Ensure you are up to date with mandatory Safeguarding and Information Governance training. If any aspect of a call raises concerns do not release any information, end the call, and seek advice.
- It is acceptable to give your name and the name of the organisation/hospital when you answer the call. You must then verify the caller.

- If the call is from a patient, check their identity by asking for three details such as their date of birth, postcode, and the first line of their address and checking these against the Electronic Patient Record. Only if this Positive Patient Identification step is completed can you disclose any information.
- If the caller is asking for information about a patient you must satisfy all these checks before disclosing any information:
    - check three details about the patient such as their date of birth, postcode, and the first line of their address and checking these against the Electronic Patient Record.
    - check that the caller is authorised to receive information about that patient. This might be because the caller is listed on the Electronic Patient Record as the next of kin, as having power of attorney, as having parental responsibility, or the caller can give an agreed password or evidence of being a member of the care team to receive an update about an inpatient.
    - If the caller is from another organisation, such as the police, ask them to put their request for information in writing so that a manager can consider the request before deciding whether to release information.
    - Bear in mind any Safeguarding alerts on the patient record. If a caller raises suspicions then you end the call. It is good practice to notify others who may answer the telephone line or who are caring for the patient in case an unauthorised caller tries to call again.

4. Further Guidance

For further information on sharing information please read the confidentiality chapter in the Trust's IG Handbook or contact the Trust's IG Team