


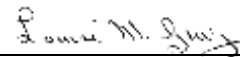



SDRN: Scottish Diabetes Research Network

SDRN & Personal Identifiable Data (PID) in Clinical Use

Clinical S.O.P. No.: 26

Version 1.0

Compiled by:	 Shona Brearley  Louise M. Gray
Approved by:	
Review date:	November 2016



SDRN & Personal Identifiable Data (PID) in Clinical Use

S.O.P. No. 26

Version 1.0

DOCUMENT HISTORY

Version number	Detail of purpose / change	Author / edited by	Date edited
1.0	New SOP	Paul McIntosh / Shona Brearley / Louise Greig	

SDRN & Personal Identifiable Data (PID) in Clinical Use

1. Introduction

ICH GCP States that 'Systems with procedures that assure the quality of every aspect of the trial should be implemented'. This SOP details the procedure to be used.

2. Background

Patient Identifiable Data includes information that the SDRN holds which can be identified to individuals and may thus breach their right to privacy or present a risk of identity theft if lost or inappropriately shared. This applies to data relating to patients, staff and any other parties. It does not apply to identifiable data already in the public domain.

3. Objectives

To describe the steps that should to be followed by the individual regarding Patient Identifiable Data. We can never overstate the importance of understanding what it is and how we are all responsible for keeping information secure.

4. Procedure

As we hold and handle Patient Identifiable Data in a number of different ways in the SDRN there are a number of rules which, if followed, will minimise the risk of losing or inappropriately sharing it.

- **Laptop & tablet computers:** These must all be encrypted. If you have doubts about the encryption status of any laptops within your service, contact your local IT Helpdesk.
- **Paper Diaries & PDAs (Personal Digital Assistants – i.e. 'Palmtop' computers):** By their nature Diaries and PDAs carry Patient Identifiable Data required for working purposes. Each staff member, as the person in control, is responsible for the security of their own diary/PDA. You must limit to an absolute minimum necessary any Patient Identifiable Data you have in Diaries and PDAs. PDAs must be password or PIN protected – contact your local IT Helpdesk for support and instructions if necessary. Unfortunately PDAs, other than **Blackberries**, are not encryptable.
- **USB (Data) Sticks:** You must only use encrypted USB sticks. If you require an encrypted stick you must apply for one via your NHS IT Help Desk. If you do not know who your Data Custodian is ask your manager/team leader.
- **Confidential paper information**, including health and staff records or correspondence, must be stored in secure locations and locked away when not in use i.e., locked file cabinets, cupboards or desks, locked rooms – not left on desks or on view through windows. All health records must be tracked/traced using the agreed locally implemented procedure.

SDRN & Personal Identifiable Data (PID) in Clinical Use

- **Sending Patient Identifiable Data:** In order to send/receive Patient Identifiable Data you must use either:
 - **Post:** For sensitive data or correspondence with multiple data subjects:
 - **External:** Please make sure the package is securely taped to prevent the contents from moving in transit and tearing the envelopes/ packaging. It is required to be double wrapped in stout envelopes/packaging with recipient and sender name and address written/printed on both layers. Envelopes/packages must be sent by Royal Mail “Special Delivery” or private courier.
 - **Internal** Use the same packaging process as mentioned above; and send to a named individual. Request an acknowledgement of delivery.

(Routine clinical or staff correspondence can be sent by ordinary mail but always assess risks to determine if a more secure delivery method is needed)
 - **NHSmail:** All staff should set up an NHSmail account and select addressee from the search function or your own contacts list to ensure recipient is correct, rather than typing into address line.

Any breach of these rules **MUST** be reported as an incident to the SDRN Co-ordinating office.