Southern Ultrasound Ltd.

42 Ascension Road. Romford. Essex. RM5 3RT Telephone: 07949 053377

Storage and Transfer of Personal and Sensitive Information

Contents

Introduction 1
Definitions 1
Policy Details 2
Patient Records: 2
Office Records: 2
Loss of Records: 3
Transfer of Information to a third-party 3
Audit & Monitoring 3
Distribution and Awareness Plan 3
Equality Impact Assessment 3
Approval 3

Introduction

All organisations have a common-law duty as well as a specific requirement under the Data Protection Act 1998 to ensure that all transfers of personal and sensitive information (correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal or sensitive information) are conducted in a secure and confidential manner. This is to ensure that information is not disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated to, within or outside of the organisation.

The loss of personal information will result in adverse incident reports which will not only affect the reputation of this organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence.

Definitions

Personal Information. This relates to 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 items 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.

Sensitive Information. This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, information defined as sensitive under the Data Protection Act 1998, eg an individual's bank account details are likely to be deemed 'sensitive', as are financial and security information about an organisation.

Policy Details

At **Southern Ultrasound** we have strict guidelines on how staff record, store and transfer personal information; whether this represents information relates to; patients we scan with in our various NHS Ultrasound services, customers obtaining goods through our healthcare consumables and equipment websites or material obtained through any other means.

Our procedures are designed to meet the requirements of the Data Protection Act, NHS Code of the Practice - Confidentiality, and the NHS Care Record Guarantee for England.

All staff are taught to work in accordance with 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 the law
- Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality (Additional principle added at 2nd review in 2013)

This policy does not affect the duty to share information for care purposes. This duty was re-asserted by the Caldicott 2 Review Panel in their report 'Information - To share or not to share: The Information Governance Review'.

The new Principle 7, states that the duty to share information can be as important as the duty to protect patient confidentiality. This means that health and social care professionals should have the confidence to share information in the best interests of their patients/service users within the framework set out by the Caldicott Principles.

Patient Records:

Hard copy patient information (including appointment letters) are handled by the NHS Trust staff and procedures rather than by the Company

With-in the Acute Hospital setting, Southern Ultrasound complies with the local rules of the Trust to ensure all records are handled correctly and in strict compliance with the NHS Care Record Guarantee for England.

NOTE: Information obtained, recorded or transmitted as a direct consequence of our contracted work for Frimley Health NHS Foundation Trust, or any other NHS Trust, will necessarily be shared with the Trust. Such transfers will be considered as an Internal transfer.

Email is not a secure system. All staff using email have been made aware of this during their induction training. Therefore, patient identifiable and other sensitive information is not sent by email unless it has been encrypted to standards approved by the NHS. NHS-mail accounts are encrypted to NHS-approved standards and may be used for sending patient identifiable information to recipients that also have an NHS-mail account.

All company staff are provided with an NHS-mail account

Electronic Information related to patient examinations and other health records are not held by the Company but retained on an NHS Trust-owned service at the clinical location. The drive has password protected, AES 256 encryption and kept in a locked location with restricted access. An off-site back-up copy is maintained in similar circumstances in a geographically different location.

Office Records:

All paper waste is shredded (cross-shredder) prior to being disposed of.

All websites, computers and Servers are password protected and have the latest antiviral software incorporated (with updates when available).

Loss of Records:

All records are securely archived, with off-site back up. Internal loss can be rectified from the off-site store with in 24 hours.

Loss of patient records in transit, or where there is a suspicion that the record has gone to an unintended receiver, will be classed as a Clinical Iincident and investigated through that format.

Transfer of Information to a third-party

See separate procedure for transfer of information to a third-party.

Procedure for Transfer of Personal and Sensitive Information to a Third Party

NOTE: Information obtained, recorded or transmitted as a direct consequence of our contracted work for Frimley Health NHS Foundation Trust, will necessarily be shared with the Trust. Such transfers will be considered as an Internal transfer.

POLICY STANDARDS

Audit & Monitoring

The Board of Directors will monitor the use of this policy and the impact of VIP visitors and on service provision.

Distribution and Awareness Plan

All staff are made aware of the policy as part of their induction training. If there are any significant changes to the policies that affect the way in which staff initiate or respond, these are communicated to them via team briefs and staff meetings.

A copy of the policy is available to all staff via the Company's on-line Governance Framework folder, and can be accessed 24/7 from any location with Web Access. A hard copy version is retained at all sites of operation.

Equality Impact Assessment

An Equality Impact Assessment has been performed on this policy and procedure. The EIA demonstrates the policy is robust; there is no potential for discrimination or adverse impact. All opportunities to promote equality have been taken.

Approval

This policy has been approved by the undersigned and will be reviewed annually and any time there is a change in the Law or guidance recommendations.

Policy Created.	13/09/18	Policy reviewed & amended:	v1
	Authorised by:	Kevin Rendell.	Director & IG Lead