Southern Ultrasound Ltd.

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

Confidentiality Audit Policy and Procedure

Contents

Version Control

v1	24/09/18	policy creation

Policy Purpose

This document defines the procedure for carrying out audits relating to access to patient level information for Southern Ultrasound

The purpose of this policy is to ensure that staff only access the records of patients with whom they have a legitimate work-related relationship or there is a legitimate business reason, and to meet the requirements of the NHS Care Record Guarantee.

Aims and objectives

The objective of this procedure is to:

- ensure that only appropriate staff access patient level information,
- Preserve Integrity
- Protect the Company's network from unauthorised or accidental modification of the Company's information;
- Preserve Confidentiality
- Protect the Company's information against unauthorised disclosure.

Scope

The procedure applies to all staff who work for Southern Ultrasound (including those on temporary contracts, contractors & agency staff).

NOTE: Southern Ultrasound does not currently receive or store patient identifiable information to its company offices, so in reality the policy is restricted to staff on the clinical site – however, the possibility of changes in the future means they have not been restricted from this policy, which has therefore been extended to include all those who have access Southern Ultrasound' patient information systems. It also applies to relevant people who support and use these systems.

With in the NHS Trust site, however, IG audit will be the responsibility of the NHS Trust itself, since it is their systems in use, and it would be inappropriate and unlawful for Southern Ultrasound to run its own audit on that information security. If and when, Southern Ultrasound operates any IT system of its own, the following shall be applied.

Roles & Responsibilities

The Director(s)

Responsible for ensuring that the confidentiality of all patient information systems is maintained and that systems, procedures & supervision is in place to achieve that end

The Information Governance Lead

The task of IG Lead has been allocated to the Company Director, who is responsible for the review and approval of this procedure.

Caldicott Guardian

The Company's Caldicott Guardian has responsibility to advise of the use of confidential data

Managers

Managers are responsible for ensuring that they and their staff are aware that confidentiality audits take place and the content and understanding of all relevant policies including but not exclusive to those relating to Information Governance.

Procedure

Access to Regular Audit Trails

The Information Governance Lead will, at least once every month, run the Audit Trail for a critical system holding patient level information at Southern Ultrasound.

If an audit trail functionality is not built into the system then a manual trail will be conducted.

The Information Governance Lead will decide which systems audit trail to run at any particular time.

Information to be contained in the Audit Trail

The information to be contained within the audit will contain at minimum of one of the following dependent on the ability of the software package: -

- Inappropriate access to a record without having the working requirement to do so;
- Repeated failed attempts to access confidential information;
- Successful access of confidential information by unauthorised persons;
- Evidence of shared login sessions/passwords

Special attention will be paid to staff attempting to access their own or other family / friends' information, safeguarding issues and patients who are considered to be *very important persons (VIPs).*

Reporting

If there are any suspicious findings from the audit trail these will be immediately reported to the Caldicott Guardian, the SIRO and remaining Company Directors, who will decide if further investigations should be carried out or if disciplinary action is required to be taken

The Information Governance Lead will produce regular reports highlighting the finding of the confidentiality audits.

Policy Implementation Plan

The Information Governance Lead

The Information Governance Lead will be responsible for the implementation of this policy.

The progress in implementing this policy will be reviewed by the Board of Directors.

Implementation Method:

Posting on the document area of the Company's Internet sites.

Publishing this policy in each of the Company's Policy Manuals.

Including reference to this policy in the IG section of staff induction and staff briefings.

Monitoring and Review

The effectiveness of this document will be monitored through on-going analysis of audit reports and the Information Governance Leeds reports to the Board of Directors.

The Policy shall be reviewed annually

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.

Review & 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.

Created	24/09/18	Last Reviewed (Annually)	v1
Kevin Rendell.	IG Lead.