Southern Ultrasound Ltd.

Southernultrasound

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

Information Security Assurance & Risk Management Plan

Table of Contents

Version Control

v1	24/09/18	Policy Creation

Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of Southern Ultrasound.

There needs to be a comprehensive programme of activity across the Company to identify information risks and manage them effectively. From the outset this needs to be recognised as an ongoing activity. A number of key activities in the Data Security and Protection Toolkit form the basis of building an information risk framework, namely:

- Mapping flows of information
- Identifying and maintaining a register of key information assets
- Setting out continuity plans for periods of information unavailability

Information Security Management Responsibilities

Information Governance Lead

The key player in the Company's Information Security Management is the IG Lead, who will, due to the small nature of the Company, also act as Senior Information Risk Owner

The IG Leads' responsibilities include:

- Managing the Information Governance agenda across the Company. This will include monitoring compliance with those requirements around Information Risk Management within the IG Toolkit and ensuring that these standards are met.
- Oversight and assurance of the processes for the identification and assessment of information risk.
- Day to day responsibility for review and maintenance of the Information Security Management System.

Acting as the SIRO, responsibilities include:

- Taking ownership of the Company's Information Risk Policy
- Acting as advocate for information risk on the board and ensure the board is adequately briefed on information risk issues
- Providing advice to the Board of directors on the content of their Annual Governance Statement in regard to information risk
- Undertaking and pass appropriately accredited strategic Information Risk Management training
- Ensuring that the Company's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Providing a focal point for the resolution and/or discussion of information risk issues

The above roles will be supported by the Company's Caldicott Guardian.

Information Asset Owner

The IG Lead also acts as the Information Asset Owner (IAO) and as such will be required to:

- Ensure the confidentiality, integrity, and availability of all information that their system processes and protect against any anticipated threats or hazards to the security or integrity of such information.
- Undertake information risk assessments on all information assets where they have been assigned 'ownership', following guidance from the Information Security team on assessment method, format, content, and frequency.
- Reporting security incidents and ensure that the reports are fully documented including type of incident and countermeasures put in place.

- To ensure countermeasures are discussed and implemented in conjunction with security incidents after consultation with the Board of Directors.
- Initiating the necessary disciplinary action if a member of staff is found to be disregarding procedures which could result in a security incident.
- Liaising with Board of Directors if incidents occur which may result in termination of employment.
- Ensure that policies and procedures are followed, including data sharing agreements
- Recognise potential or actual security incidents
- Ensure that information assets registers are accurate and maintained up to date.

All Staff

Each Company staff member, including any external contractor working on behalf of the Company, has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate treatment actions. Training will be provided for all staff to enable them to ensure that information assets registers are accurate and maintained up to date

The Information Security Management System

An Information Security Management System (ISMS) system has been developed which encompasses:

- Information Asset Register (including risk assessments)
- Person Identifiable Data Flow Mapping
- Identification of critical assets (business impact assessment)

This is the central tool used by the IG Lead and the information collected within the ISMS supports 6 of the 28 requirements of the IG toolkit, as well as the organisation's work towards International Security Standard: ISO27001.

It is planned that the ISMS will be developed further over the next 12 months to include the following modules:

Full Person Identifiable Data Flow Mapping – to collect all relevant information regarding data transfers and risk assessment of those transfers

- Register of Info Sharing Agreements
- Control of access to Info Assets
- Corporate Records Audit
- Application and Database Register
- Safe Haven Fax Audits & Directory
- Management of Portable Media

Information Assets

Information assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation, such as:

- databases
- data files
- contracts and agreements
- system documentation
- research information
- user manuals
- training materials
- operational/support procedure
- business continuity & back-up plans
- audit trails
- archived information

Information assets could be kept in a variety of formats and on a variety of media, e.g. paper, on a computer drive or network, on removable media (e.g. USB memory sticks, CD-ROM).

Information assets may contain person identifiable or commercially sensitive information.

Identification of Information Assets

Entry of new Information Assets on to the Information Asset Register section of the ISMS will be performed at the time of acquisition, and checked annually. Systems removed from active use will not be removed from the register until at least 12 months after their complete destruction has been assured.

Risk Assessment

The Information Asset Register will be used to calculate a general risk assessment for each information asset that is entered into the register. A likelihood, consequence and therefore overall risk score will be calculated based on the information provided regarding the information contained in the asset and how the asset is stored.

Further to this, the IG Lead will assess the worst-case scenario of the possible effects the loss of confidentiality, integrity and availability of each information asset would have to the business, including financial, adverse publicity, relationship with patients or NHS and the risks associated with non-compliance to legislation. This is achieved by the IG Lead selecting the most appropriate statement from a list of five, each derived from the Company's risk matrix and relating to a consequence score of 1 to 5. This process will allow "critical" assets to be identified and can provide the basis of this component of the company's business continuity plans.

Maintenance

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the information assets held by the organisation and the risks associated with them, resulting in a requirement to review any previously recorded information assets and risk assessments. Consequently, the information asset register shall be subject to regular maintenance by the IG Lead.

Person Identifiable Information Flow Mapping

In our work for the NHS, numerous urgent and routine transfers of patient and staff information take place each day for the purposes of healthcare and administration of healthcare services e.g. letters to patients, e-mails to clinicians, moving case notes.

It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation.

To ensure all transfers are identified, the Company must determine where, why, how and with whom it exchanges information. This is known as Information Flow Mapping and the comprehensive register provided by this exercise identifies the higher risk areas of information transfers requiring effective management. It also allows any Information Sharing Agreements that should be in place to be identified.

To adequately protect transfers/flows of information, the Company must identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with the Company's Safe Haven Procedures as explained in the Information Security Procedures and relevant legislation (e.g. Principle 7 of the Data Protection Act 1998 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data).

The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence. Fines of up to £500,000 may be imposed by the Information Commissioner's Office on organisations and individuals within organisations that do not take reasonable steps to avoid the most serious breaches of the Data Protection Act.

Identification of Information Flows

The information recorded in the Information Asset Register allows the identification of all assets of which part or all of their content are sent or received either internally or externally to the Company.

Further development of the ISMS in will allow a "Data Flow Mapping" module to be added which will collect information about how and where the information is transferred, and risk assess this data within the ISMS.

As with the Information Asset register, person identifiable information flows are subject to change and therefore will be reviewed regularly. A formal review will be conducted at least annually.

Information Incident Reporting

Damage resulting from potential and actual information security events should be minimised and lessons learnt from them. All security incidents, suspected or observed, should be reported, recorded and investigated and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur. This includes weaknesses identified in systems design or operational procedures that potentially may result in an information security incident.

All members of staff have the responsibility to report all information incidents and near misses that they observe, unless they are aware that the incident has already been reported.

All staff are required to report incidents and near misses promptly and to ensure that the information they give provides an accurate account of the incident so that follow up action can be taken. Managers are required to review and approve incident reports promptly and manage incidents to update completed actions and clear outcomes.

Purpose of the Confidentiality Audit

The DSP Toolkit requires that organisations ensure access to confidential personal information is monitored and audited locally, and in particular ensure that there are agreed procedures for investigating confidentiality events.

The Company has processes to highlight actual or potential confidentiality breaches, particularly where person identifiable information is held and must also have procedures in place to evaluate the effectiveness of controls within these systems.

Southern Ultrasound already has a comprehensive range of control mechanisms in place to manage and safeguard patient confidentiality. This document will establish appropriate confidentiality audit procedures to monitor access to confidential personal information throughout the Company.

This work forms part of the Company's overall assurance framework and meets requirements within:

- the NHS Care Record Guarantee
- the NHS Information Governance Toolkit
- the Healthcare Commission core standards
- the NHS Confidentiality Code of Conduct
- Registration Authority Governance Arrangements for NHS Organisations

Confidentiality audits will focus primarily on controls within electronic records management systems, but will not exclude paper record systems: the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of weak, non-existent or poorly applied controls.

For full details, see separate policy:

Confidentiality Audit Policy & Procedure

Training

It is now mandatory for all NHS staff (including those working through contract such as Southern Ultrasound' staff) to undertake IG training, on an annual basis.

The Connecting for Health IG Training Tool is an online training tool developed and improve staff knowledge and skills in the IG work area.

Following the Training Needs Analysis conducted in relation to requirement 134 of the IG Toolkit, it was decided that all staff **must** initially work through the relevant module, marked as mandatory in the training tool, and pass the accompanying assessment:

- All staff with routine access to personal information - '**Introduction to Information Governance**'
- All other staff - '**Information Governance - The Beginner's Guide**'

If one of these modules has already been completed, then the refresher module must then be completed annually.

Further Information Risk and ISMS system training will be made available as deemed suitable by the IG Lead. The training will provide an understanding of what information assets are and how they are to be recorded and risk assessed in the Information Security Management System (ISMS) will be given.

Reporting

The SIRO will receive quarterly reports that highlight all information risks across the Company. A decision will then be made about whether this is a risk that the organisation will accept or take measures to control. The reporting structure is a constant cycle ensuring escalation and feedback at all stages of the Information Risk Process.

Related Policies

This plan should be read in conjunction with the following policies:

- Comprehensive Information Governance Policy;
- Information Security Incident Policy
- Information Security Incident policy
- Confidentiality Audit Policy & Procedure

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.

Plan Creation:	24/09/18.	Last amendment & review:	v1 N/A
Kevin Rendell	Director & IG Lead		