Comprehensive Information Governance Policy

Contents:

Introduction

Southern Ultrasound recognises its responsibility to respect and protect the privacy of its users, not least because of the sensitive information we obtain and record by way of patient medical records, and will strive to achieve and promote best practice throughout its business activity.

To guide us in this endeavour, we have created a collection of Policies and supporting Procedures including:

- A Clinical Governance Policy, of which this Information Governance Policy is a Key feature
- A Confidentiality Policy, to comply with the Data Protection Act 1998 and other legislation
- A Patient Record Guarantee – taking key relevant aspects of the NHS Care Record Guarantee
- An IT Security Policy suite – to ensure the physical security of equipment and information.

Responsibility for Information Governance is held by the Company's Information Governance Lead – Kevin Rendell

Staff Training

In order that **Southern Ultrasound** maximise the effectiveness of their Information Governance; we need to ensure that all staff are fully aware of the principles and policies around Data Protection, Information security and Confidentiality.

This is achieved by placing Information Governance at the centre of our activities, to be discussed with staff at training events, appraisals, case reviews and staff meetings.

All staff shall be required to complete an approved Information Governance training course on an annual basis. This may be a face-to-face or IT provided course. Certification shall be retained in the staff records.

The **Southern Ultrasound** 'Information Governance Lead' shall have responsibility for ensuring Information Governance is kept as a priority in all Company activities and for raising any concerns at board level.

Both the **Southern Ultrasound** 'Information Governance' Lead and 'designated Caldicott Guardian' shall liaise with all staff to ensure they are kept aware of any developments in procedures and act as a conduit for staff to raise any concerns or queries

Principles of information security

The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. This includes both Patient records and staff records. In the case of the NHS, the most sensitive of our data is patient record information.

In practice, this is applied through three cornerstones - **confidentiality, integrity and availability**

1. Information must be secured against unauthorised access - **confidentiality**
2. Information must be safeguarded against unauthorised modification - **integrity**
3. Information must be accessible to authorised users at times when they require it - **availability**

Information Governance is there to ensure these principles are upheld by setting clear guidelines (policy) for all users.

More importantly, Information Governance provides guidance and an update to the contractual controls that protect patient, system and employee information.

Without these contractual controls there is no way for the NHS to support, through legal action, human rights, data protection or other forms of regulation, the levels of protection we all work so hard to maintain.

Data Protection principles

The following principles apply to both all health record data and to general personal data:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Policy Overview

Information Governance (IG) cannot be regulated and monitored with a single policy. **Southern Ultrasound**' therefore has a range of individual policies which often need to be read in conjunction with each other.

The following pages collect all these policies together in a single document, giving the reader a single location to access all the required information.

Where possible, the policies have been arranged with a common theme, but it must be appreciated that there is a good deal of overlap between various elements of IG and therefore the user might need to access multiple sections of the document for a comprehensive appraisal of relevant policies.

To ease access, the policy titles shown on the contents page are hyperlinked to the relevant section.

This document contains only the IG Policies, and does not include Management Frameworks, Strategies & Plans, IG Procedures (except where incorporated into a Policy), Check lists or Assessments.

System Level Security Policy

Introduction:

The development, implementation and management of this System Level Security Policy (SLSP) is designed to help the Company to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of Information system.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of patient identifiable / sensitive data.

Current Encryption guidance for health and care organisations can be found at https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/encryption and it is expected that any electronic solution for the handling of patient identifiable / sensitive data to comply with this guidance as a minimum..

*The SLSP is a core component of **Southern Ultrasound** Information Governance policy schedule supporting the Company's formal accreditation processes for its information assets.*

System Details

- **Southern Ultrasound**' information Assets represent an essential and vital Company System, fundamental to its operations.
- The Systems' responsible owner is The IG Lead,

Policy Details

The SLSP is a core component of **Southern Ultrasound** Information Governance policy schedule supporting the Company's formal accreditation processes for its information assets.

Our full suite of NHS Digital approved IT polices should be read in conjunction with this SLS Policy.

System Security

- Security of the system shall be governed by the Board of Directors
- The System's responsible security manager shall be the IG Lead. The IG Lead is responsible for accrediting the system's security implementation.
- Security training will be provided to the IG Lead through the IGTT
- The System incorporates the following security countermeasures….
    - Hard copy information is converted to digital format as early as possible.
    - All electronic components of the system are protected by 256KB encryption, with password protection.
    - All electronic components of the system are protected by complete and continuously updated anti-virus software and system management software.
    - There is regular system wide audit.
    - This policy shall be reviewed annually

Confidentiality Code of Conduct

Southern Ultrasound shall ensure its operations comply with the current "Code of Practice on Confidential Information", and shall promote this code to all staff.

See https://digital.nhs.uk/cop & https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

(**NOTE**: Although this code was written by the now superseded 'Health & Social Care Information Centre', it remains in force until NHS Digital or some other body feels circumstances have changed sufficiently for it to be rewritten).

shall ensure its operations comply with the current "Code of Practice on Confidential Information", and shall promote this code to all staff.

See https://digital.nhs.uk/cop & https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

(NOTE: Although this code was written by the now superseded 'Health & Social Care Information Centre', it remains in force until NHS Digital or some other body feels circumstances have changed sufficiently for it to be rewritten).As per that code:

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It –

a) is a legal obligation that is derived from case law;

b) is a requirement established within professional codes of conduct; and

c) is included in **Southern Ultrasound** employment contracts as a specific requirement.

Full details are available in the NHS Code of Practice on Confidential Information and a copy of this code has been provided to all staff and is available in the 'Information Governance' sub-folder of the 'Information For Staff and Contractors' folder of our online 'Quality Assurance' system.

To fulfil these obligations,

- Staff shall ensure that Personal data is processed lawfully, with confidentiality seen as a key parameter
- Staff shall ensure that Personal data is used only for the purpose for which it was provided, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Staff shall ensure that Personal data is adequate, relevant and accurate and make every effort to ensure it is kept up to date, by confirming relevant aspects when in contact with the patient and amending the records as necessary.
- Staff shall not access records which are not relevant to their work roll or current patient requirements.
- When requested, staff shall inform enquirers how patients may access their records and forward all requests for patient access to their records, to the Caldicott Supervisor or IG Lead.
- Staff shall follow company procedures to ensure that records are kept confidential and prevent access by others. This includes correct storage on encrypted drives, correct shredding of hard-copy files, use of password protection and informing management when they believe records have been accessed inappropriately or unlawfully.

Confidentiality Audit Policy and Procedure

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 and Information Governance Toolkit (IGT)

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/Supervisor

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

Managers

Managers are responsible for ensuring that 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

Storage and Transfer of Personal and Sensitive Information

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.

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 Detail.

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'.

A 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 (other than appointment letters) is not posted in the general post and appointment letters do not include any Sensitive information. Examination reports are handed direct to the patient and/or sent via surgery drop numbers.

When a patient record has to be faxed to a GP Surgery, for instance when an urgent examination report is requested, they are only faxed to the surgery fax number provided by the Clinical Commissioning Group and the fax number is confirmed by two members of staff to avoid issues as a result of input errors.

Within 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.

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. NHSmail accounts are encrypted to NHS-approved standards and may be used for sending patient identifiable information to recipients that also have an NHSmail account.

Electronic Information related to patient examinations and other health records is held on a hard-drive completely isolated from the internet and without WiFi capabilities. 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). Both incoming and outgoing emails are vetted through "MessageLabs" to ensure malicious content is neither received nor propagated.

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 records in transit, or where there is a suspicion that the record has gone to an unintended receiver, will be classed as a Clinical incident 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.

Physical and Environmental Security Policy

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 the Company.

Southern Ultrasound' acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Company's Security Policy, Security Standards and Work Instruction Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Company. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Company.

This procedure outlines how the Company maintains a controlled working environment.

Environmental Security

The Directors have overall responsibility for Facilities Management, although selected aspects might be delegated to individual Staff members or teams as decided applicable to the Board at the time

Whilst the Company maintains Employers Liability Insurance and Public Liability insurance, Health and Safety is the responsibility of every individual and their line manager.

Our clinical sites are owned and operated by 3rd-parties' Eg Frimley Health NHS Foundation Trust, and all staff working in such locations must be aware of, and follow, the Local Rules, including those on Security and safety.

The Company has procedures in place for Emergency Response and Business Continuity.

Physical Security Policy

As a small company, **Southern Ultrasound** staff are generally required to 'multi-task' and operate with a wide overlap of job responsibilities. All staff therefore require variable access to all Company areas and all Company systems. For this reason, the Company does not demarcate specific physical areas of increased security, nor restrict access to any of its systems to any of its staff.

Staff have, however, been informed via team brief, and within the terms of their employment contract, that they are only authorised to access information and/or information asset systems for the purpose of their work role, and are required to limit such access solely to the minimum access required for that particular task.

Access to Information Assets is logged and regular audits are processed.

Access to information assets by contractors is restricted to the systems in use for their work role.

Staff are advised to challenge or report any person who they believe to be in an unauthorised location or accessing information or other Company systems without similar authorisation.

Mobile Systems

Mobile computing systems are identified with in the Asset Register and are security marked with indelible ink confirming ownership. Their hard-drives are encrypted and password protected ensuring access is restricted to authorised staff.

Staff have been instructed on the use and storage of mobile equipment, including security issues and privacy matters such as ensuring the monitor is only visible to authorised viewers and not left on when unattended. Patient identifiable information is NEVER stored on Southern Ultrasound's portable equipment.

IT issues

In the case of any of the following issues with any information asset or other Company system, staff are required to contact a Senior Manager or Company Director without delay:

- Failure to power-up of a Computer desktop, laptop or other Information System.
- Failure to connect to the network, using personal account name and password.
- Any system failure or unexpected restart, during operation of an Information System.
- System notification of absent or impaired function of anti-virus or system monitoring software.
- System notification of improper operation, corrupted hard-drive or driver update required.
- Any other abnormal function of the system.

All PC's are turned off at night, unless local rules contradict this requirement.

The Company Servers are surge protected, and externally monitored and backed-up. They are maintained by a third-party IT support company (Global IT Solutions Ltd) and staff are not authorised to access any part of the server, either physically or electronically, other than to authorised drives via their work-station for the purpose of their daily work role.

Equipment Location and Protection

In accordance to the Health and Safety Act, the Company has positioned all equipment with due consideration. (In clinical sites, this has ben agreed in conjunction with the site providers.

Consideration has also been given to the protection of information available from it.

Should any member of staff require the repositioning of equipment, permission must be obtained from the Senior Management.

Cabling is laid within appropriate trunking. All cables are tied and secured in the office environment, no cables will be laid across open floors as these are hazardous and could cause an employee to trip.

It is the employee's responsibility to ensure that any computer equipment that has been provided to them solely for their use remains in the same condition as it was when provided. Disciplinary action may be taken against personnel if any case of misuse against equipment is found.

It is the responsibility of every employee to report any fault to do with the infrastructure to Senior Management so that a decision can be made as to whether the problem can be rectified internally, or whether it needs to be escalated.

Any security incidents, hardware or software failure must be documented and reported providing information of the status, even if the problem has already been fixed, so it can be reviewed accordingly.

Protecting against Malicious Code – Training policy

Policy Summary:

Southern Ultrasound' must regularly train and remind its workforce about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

Purpose:

This policy reflects **Southern Ultrasound**' commitment to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

Policy:

Southern Ultrasound must be able to effectively detect and prevent malicious software, particularly viruses, worms and malicious code.

1. Southern Ultrasound' has developed, implemented, and shall regularly review a formal, documented process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data.

See:

- IT Policy - Anti-Virus and Malware &
- Information Governance Procedure - Protection against malicious code

All Southern Ultrasound' workforce members shall be regularly trained and reminded about these documents and processes.

At a minimum, Southern Ultrasound' malicious software prevention, detection and reporting process must include:

- Installation and regular updating of anti-virus software on all Southern Ultrasound' information systems.
- Examination of data on electronic media and data received over networks to ensure that it does not contain malicious software.
- The examination of all electronic mail attachments and data downloads for malicious software before use on Southern Ultrasound' information systems.
- Procedures for members of the workforce to report suspected or known malicious software.
- An appropriate disaster recovery plan for recovering from malicious software attacks. Procedures to verify that all information relating to malicious software is accurate and informative.
- Procedures to ensure that Southern Ultrasound' workforce members do not modify web browser security settings without appropriate authorization.
- Procedures to ensure that unauthorized software is not installed on Southern Ultrasound' information systems.

2 At a minimum, Southern Ultrasound' protection from malicious software training and awareness must cover topics including, but not limited to:

- How to identify malicious software.
- How to report malicious software.
- How to effectively use anti-virus software.
- How to avoid downloading or receiving malicious software.
- How to identify malicious software hoaxes.

Unless appropriately authorized, Southern Ultrasound' workforce members must not bypass or disable anti-virus software.

References:

- **Southern Ultrasound**' IT Policy - Anti-Virus and Malware and
- **Southern Ultrasound**' Information Governance Procedure - Protection against malicious code

Records Management Policy

Introduction

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal.

The Records Management: NHS Code of Practice© has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

Southern Ultrasound' records form a significant part of its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Company and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The Board of Directors has adopted this records management policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced costs.

The Company also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

This document sets out a framework within which the staff responsible for managing the Company's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

This policy document should be read in conjunction with the Company's Records Management Strategy which sets out how the policy requirements will be delivered.

Scope and Definitions

This policy relates to all clinical and non-clinical operational records held in any format by the Company. These include:

- all administrative records (eg personnel, estates, financial and accounting records, notes associated with complaints); and
- all patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Company and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

The term **Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the Company in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

Information is a corporate asset. The Company's records are important sources of administrative, evidential and historical information. They are vital to the Company to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

Aims of our Records Management System

The aims of our Records Management System are to ensure that:

- **records are available when needed** - from which the Company is able to form a reconstruction of activities or events that have taken place;
- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so all staff are aware of their responsibilities for record keeping & management.

Roles and Responsibilities

The **IG Lead** has overall responsibility for records management in the Company. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

The Company has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

The Company's **Caldicott Guardian/Supervisor** has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

The Company's **Records Manager is** responsible for ensuring that this policy is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated and monitored. They are also responsible for the overall development and maintenance of health records management practices throughout the Company, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information. Within **Southern Ultrasound** the responsibilities of the Records Manager are rtaken by the IG Lead.

All Company staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Company and manage those records in keeping with this policy and with any guidance subsequently produced.

Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The Company will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

and any new legislation affecting records management as it arises.

Inventory of Record Collections

The Company will establish and maintain mechanisms through which teams can register the records they are maintaining. The inventory of record collections will facilitate:

- the classification of records into series; and
- the recording of the responsibility of individuals creating records.

The inventory will be reviewed annually.

Retention and Disposal Schedules

It is a fundamental requirement that all of the Company's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Company's business functions.

The Company has adopted the retention periods set out in the Records Management: NHS Code of Practice (detailed in the Company's Retention Schedules for Health and Non-Health Records). The retention schedule will be reviewed annually.

Records Management Systems Audit

The Company will regularly audit its records management practices for compliance with this framework.

The audit will:

- Identify areas of operation that are covered by the Company's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Company Board.

Training

All Company staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance initiated as from their Induction.

Loss of Data

Any, suspected or confirmed, loss of data represents a serious incident and should be immediately reported under the company's Clinical Incident Reporting policy. The Company's Information Governance Lead shall perform a full investigation in consultation with the Caldicott Guardian to minimise the loss, avoid any repetition or similar loss, make recommendations on staff training needs and make decisions on the need to advise relevant 3rd parties.

Home Working Policy and Procedure

Policy objective:

To manage and prevent unacceptable risks arising to the organisation and other NHS information assets through the use of unapproved or unsafe home working facilities.

Scope:

All staff who are permitted to use equipment of the organisation at home or who may use their personal computing resources to connect to networked services of the organisation are subject to the requirements of this IG policy and procedure.

Responsibilities:

Home Working is only permitted with the express agreement of the Board of Directors, who will also decide upon the extent and limitations of such work.

The IG Lead is responsible for the local definition of network, infrastructure and PC information security requirements and for the supply and configuration of all computing equipment provided by the organisation. This will include network connectivity and support for approved services.

Where, exceptionally, agreement is provided that a home worker may use their personal computing resources for a business purpose of the organisation, the IG Lead and IT security manager must be satisfied that the resources concerned are configured appropriately, that the security measures are implemented and operating correctly and that no unacceptable information governance risks exist.

The IG Lead is responsible for ensuring that a home risk assessment survey is conducted where necessary and for the identification of any necessary improvements or controls that affect the proposed home work area. In addition, the IG Lead will provide guidance to the home worker on all relevant security policies and responsibilities.

Home Risk Assessment Survey:

A home risk assessment survey will be necessary when an individual who regularly works from home, (defined as at least 6 times during a year), has access to:

- Documents protectively marked as 'confidential' or above in accordance with central government guidelines;
- other commercially or otherwise sensitive documents;
- any sensitive person identifiable information about patients or staff;
- person identifiable information about patients or staff deemed non sensitive but still significant in terms of quantity (defined as 50+ records)
- anonymised information about patients or staff unless the anonymisation technique has been approved by the organisation's Caldicott Guardian.

Unless instructed otherwise, the home worker is responsible for ensuring that their home contents insurance cover extends to all provided equipment belonging to the organisation.

IG Security Procedures for home working:

The home worker's proposed working environment(s) should be considered and where necessary surveyed, and any perceived IG risks assessed to help inform consideration of home working options. The findings of this consideration or survey process and any associated risks should be documented, so that appropriate control measures may be reviewed.

Where the proposed home working arrangements involve the use of personal or shared computing resources, it must be noted the IG risks of doing so may outweigh any operational advantage of home working. For all home working scenarios, consideration of risks must be made and should take account of the potential to:

- accidentally breach patient confidentiality;
- disclose other sensitive data of the organisation to unauthorised individuals;
- lose or damage critical business data;
- damage the organisation's infrastructure and e-services through spread of un-trapped malicious code such as viruses;
- create a hacking opportunity through an unauthorised internet access point;

- misuse data through uncontrolled use of removable media such as digital memory sticks and other media;
- cause other operational or reputational damage.

When a home working agreement is possible the purpose, terms and conditions should be formally reviewed and agreed by the home worker. A reference copy of this agreement must be provided to the home worker. All such home working agreements should be reviewed periodically for their continued applicability.

Steps should then be taken to define, agree and implement the environmental security controls deemed necessary. The IG Lead should maintain records of all such assessments, surveys, related decisions, agreements and implementation plans.

It is the responsibility of the home worker to maintain their home working environment in conformance with the organisation policies and agreement permitting their home working. Where a home worker requires clarification or guidance they should consult the IG Lead

The home worker should be made fully aware of their information governance responsibilities to the organisation. Training should be provided to home workers for any additional or special tools or functions that underpin the security of their home working, including provided access and log-on tokens. Such facilities and the training in their use are the responsibility of the IG Lead. This may for example include guidance on the deletion of cached information from internet browsers used to access web-based services.

Failure by staff to observe and maintain their home working agreement may result in their home working facility being withdrawn.

It is the responsibility of the IG Lead to ensure that the organisation infrastructure is maintained in a technically secure manner that would reasonably prevent a security breach arising from a home worker's location.

Once all necessary steps have been satisfied the home working arrangements agreed may be made operational. Please note that other NHS IG codes of practice and good practice guidance for information governance security management, the use of data encryption tools and for the security of permitted removable media remain applicable and should be followed.

Audit spot checks should be considered by the organisation to ensure this home working policy is complied with and the agreement with the home worker should clearly specify that this may occur. Any compliance issues will be reported to the line managers concerned and may be handled through staff disciplinary processes or contractual arrangements.

All incidents involving the use of home working facilities must be reported to the organisation's IG Lead immediately and in accordance with the organisation's incident reporting procedures.

Use of NHS Number Implementation Plan

Introduction

The NHS Number is the national unique patient identifier that makes it possible to share patient information across the whole of the NHS safely, efficiently and accurately.

Use of the NHS Number has been mandatory since September 2009(1). It is the common unique identifier that makes it possible to share patient information across the whole of the NHS safely, efficiently and accurately. The NHS Number is classed as Personal Identifiable Data (PID) as defined by the Data Protection Act 1998.

The NHS number is the key to unlocking services such as the NHS Care Records Service, Choose and Book or the Electronic Prescription Service. It is a unique 10 digit number assigned to every individual registered with the NHS in England and Wales. The first nine digits are the identifier, and the tenth digit is a check digit used to confirm the number's validity.

The NHS Number is the only National Unique Patient Identifier in operation in the NHS and the use of this number is fundamental to improving patient safety by :

- Reducing clinical risks, caused by misallocation of patient information
- Ensuring that the patient record being viewed be a clinician is unique to the patient
- Resolving some of the barriers to safely sharing information across healthcare settings
- Assisting with long term follow-up processes and audit

How the NHS Number is allocated

Patients are allocated an NHS Number through the following routes:

- At birth
- When registering with a GP practice at the point that they first use the NHS
- At an increasing number of secondary care organisations, using the advanced functionality of the Data Spine in conjunction with the Personal Demographics Service (PDS) – but only under carefully controlled conditions.

An NHS Number will be issued once to a patient, irrespective of their entitlement to care.

Southern Ultrasound does NOT issue NHS Numbers, but it is an Information Governance requirement that service user records, both paper and electronic, have an NHS Number stored on them as early as possible in the episode of care. Staff should be routinely using the NHS Number as part of the provision of care, to link the service user to their care record, to communicate within and between the Company and NHS.

This is in keeping with National Patient Safety Guidance and the Information Governance Toolkit. This supports the main principles behind the use of the NHS Number:

- The NHS Number will be used as a patient identifier on all systems and documents which include Patient Identifiable Data
- The NHS Number will be the first choice for searching electronic patient records
- The NHS Number will be determined before or at the start of an episode of care
- The NHS Number will be supplied as a patient identifier for any Patient Identifiable Data that passes across system or organisational boundaries

Purpose

This procedure applies to all patients/clients who are referred to the Company and to all staff who create or use care records, use on-line and/or need to generate information for access to batch-tracing NHS numbers. The NHS number is a mandatory field for all existing systems (where the NHS Number is known) as it will be used to verified data to enable migration to the NHS Care Records Service.

Responsibility

The IG Lead is responsible for monitoring the use of the NHS Number and will provide regular reports on the use of valid NHS Numbers via data quality reports.

All staff are responsible for:

- Entering and checking that the NHS number, when known, is recorded in the appropriate places in all care records.
- Ensuring that the NHS number is used on correspondence, case notes, etc.

Process.

All clinical communications will display the NHS number.

The NHS Number will be used at every opportunity as an identifier for a patient this includes:

- Electronic Patient Record
- Hard Copy Patient Record
- Electronic communication relating to a patient
- All hard copy documents relating to a patient
- All labels used in administrative and clinical documents

Displaying the NHS Number

The NHS Number consists of 10 digits, the first nine digits constitute the identifier and the tenth digit is used for validation. The NHS Number should be displayed in 3-3-4 format i.e. **123 456 7890**

Accessing the NHS Number when it is not provided

Where the NHS number is not provided, the clinical staff (including support staff) will be required to ask the referring department to provide the number, as soon as the absent number is noted.

A log record of each episode where no NHS number was provided will be maintained and the IG lead will perform a monthly audit of the log to identify common issues and generate a report on NHS Number compliance.

Education and Training.

The IG Lead will monitor compliance and review training requirements and provide guidance materials for staff. Such information will be disseminated at team briefs, staff assessments and one-to-one staff training. In some cases, training will be provided via the IGTT, or it will be provided using information from the IGTT and other sources.

Monitoring and Review

Adherence to this policy and the use of NHS Numbers will be monitored through regular audits including:

- Quarterly Data Quality Reports
- Annual Clinical Records Audit
- Reporting via the Information Governance Toolkit

Pseudonymisation and Anonymisation Policy

Introduction

The aim of this policy is to enable **Southern Ultrasound**' staff to access and carry out secondary use of patient data in a legal, safe and secure manner. It is a legal requirement that when patient data is used for purposes other than direct care, i.e. Secondary Uses, the patient should not be identifiable unless otherwise legally required such as having obtained the patient's consent or Section 251 approval. This is set out clearly in the Department of Health's document 'Confidentiality: the NHS Code of Practice', which states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data.

The Data Protection Act 1998, the Human Rights Act 1998 and the common law relating to confidentiality apply to all organisations. They require that the minimum personal data are used to facilitate any particular purpose and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned unless there is a lawful exemption under the Data Protection or Human Rights Acts to do so. All NHS organisations and those working in conjunction with the NHS, such as **Southern Ultrasound**, must respect people's private lives. Pseudonymisation and Anonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses. Pseudonymisation is a core element of Secondary Uses Services (SUS) and shall be applied across the Company.

Southern Ultrasound has a legal obligation to comply with all appropriate legislation and guidance issued by professional bodies in respect of pseudonymisation and anonymisation.

This Policy outlines how the Company will meet its legal obligations and NHS requirements concerning pseudonymisation and anonymisation.

The Policy relates to roles that are reliant on computer systems and manual records such as: patient administration, purchasing, invoicing and treatment planning and the use of manual records relating to patients, staff and others whose information may be held by the Company.

Purpose and Scope

This policy applies to all **Southern Ultrasound**' staff (including substantive & temporary,) and Sub-contracted staff working through the Company, who use patient data for secondary use purposes and uses other than direct patient healthcare with guidance to safeguard the confidentiality of the patient. The policy has been developed in line with the NHS Digital and the Information for Governance Toolkit.

The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure the care provided. Where this is not practicable data should flow through business processes that minimise the risk to data. In many circumstances this requires data to be received under 'New Safe Haven' authorisation where it can be processed securely and only used in an identifiable form for specific authorised procedures within the New Safe Haven boundary. Onward disclosure should be limited to pseudonymised or anonymised data.

Planning guidance published by the Department of Health in support of the 2010/11 Operating Framework sets out clear targets:

It states that: ***"It is NHS policy and a legal requirement that patient level data should not contain identifiers when they are used for purposes other than the direct care of patients, including local flows between organisations as well as data extracted from the Secondary Uses Service.***

NHS Commissioners should ensure that organisations from which care is commissioned comply.."

Definitions

Patient/Personal Identifiable Data (PID)

Patient Identifiable Data is information about a person that would enable the person's identity to be established. This might be fairly explicit such as initials and 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.

Any of these items can be considered collectively or in isolation as patient identifiable information: Surname, Forename, Initials, Address, Date of Birth, Other dates (e.g. death, diagnosis), Postcode, Gender, Occupation, Ethnic group, NHS or Hospital Number, National Insurance Number, Telephone number and Local Identifier.

Primary use

Use of data that directly contributes to the safe care and treatment of a patient and include diagnosis, referral and treatment processes together with relevant supporting administrative processes, such as clinical letters and patient administration, patient management on a ward or GP surgery, managing appointments for care; as well as the audit/assurance of the quality of the healthcare provided is considered primary use.

Secondary use

Other uses of the data, that is the non-direct care usage referred to above, are usually known as secondary uses. Examples of secondary uses are for trend analysis, medical research, financial audit and the management of health care services, as set out in Confidentiality: the NHS Code of Practice, Ref 6.

Information Processing

Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data,
- Retrieval, consultation or use of the information or data,
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data;

Caldicott Principles

The Caldicott report relates to the use of patient-identifiable information within the NHS and highlights two key points: All NHS organisations must appoint a Caldicott Guardian, and details of six key principles to be applied when using patient–identifiable information.

Compliance with these principles reduces the risk of breach of confidentiality and breaches of legal requirements. This is best practice in accordance with the NHS Confidentiality Code of Practice (November 2003) and should therefore be adopted when implementing Pseudonymisation and Anonymisation Project.

Southern Ultrasound has an appointed Caldicott Supervisor.

Roles and Responsibilities

The IG Lead has overall responsibility for Information Governance within **Southern Ultrasound** and has a responsibility for ensuring that it meets its legal responsibilities. The IG Lead also has a responsibility for the adoption of internal and external governance requirements which oversees the implementation of the pseudonymisation and anonymisation project as per the NHS Policy.

The IG Lead is also responsible for ensuring that this policy is implemented, and that New Safe Haven processes and procedures are developed, co-ordinated and monitored to comply with the company's Information Governance Framework.

The **Caldicott Guardian/Supervisor** has a responsibility for review and authorisation of all procedures that relate to the use of patient identifiable information under the pseudonymisation and anonymisation project.

De-Identification

Staff should only have access to those data that are necessary for the completion of the business activity which they are involved in. This is reflected in Caldicott Principles; ***Access should be on a need to know basis***. This principle applies to the use of PID for secondary or non-direct care purposes.

By de-identification, users are able to make use of non identifiable patient data for a range of secondary purposes without having to access the identifiable data items.

The aim of de-identification is to obscure the patient identifying information items within the patients record sufficiently that the risk of potential identification of the respective service user is minimised to acceptable levels, this will provide effective anonymisation. The use of multiple pseudonyms should be adopted, a single pseudonym for use within **Southern Ultrasound** and a separate pseudonym for use outside of the organisation.

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets. This allows the linking of data sets and other information which is not available if the patient identifiable data is removed completely.

Where patient identifiable data is required the NHS Number must be used as part of this data set. The NHS Number should be included within all patient records and documentation in line with the current NHS Digital requirements.

Pseudonymisation

To effectively pseudonymise data the following actions must be taken:

An algorithm must be applied to the agreed field within the patient record, i.e. the NHS Number to generate a pseudonymised identification number, to be used on reports for secondary use purposes.

Each field of PID must have a unique pseudonym.

Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability.

For example; in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.

Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports.

Pseudonyms for external use must be independently generated to give different pseudonym from the one used internally in order that internal pseudonyms are not compromised.

The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines.

Pseudonymised data should have the same security as PID.

Use of Patient Identifiable Information

Patient Identifiable information must only be used for justified purposes, ***on a need to know basis*** and only by those who have been authorised to do so, via the Caldicott Authorisation to Access patient-identifiable information for secondary uses form. (Annex B)

Information Governance Requirements

Appropriate information governance arrangements must be put in place to ensure the proper use of information and maintain the security and confidentiality of information at all times.

Transferring Information

Where it has been identified that information sharing is to take place with other organisations, information sharing agreements shall be documented, agreed and signed up to by the Caldicott Guardians / IG Lead / SIRO of the partner organisations to that agreement.

Training

All staff are required to complete the statutory and mandatory information governance training on an annual basis, as directed by the IG Lead.

Staff will be made aware of this policy and its operational requirements through team brief and assessments.

The policy will be available to staff via the Company Server, and with in the Information Governance Policy book.

Review

This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

Discipline

Breaches of this policy may be investigated and result in the matter being treated as a disciplinary offence under **Southern Ultrasound**' Disciplinary Procedure.

IG Forensics Policy

The Board of Directors of Directors has approved the introduction of IG forensic readiness into the business processes and functions of the Company. This should maximise its potential to use digital evidence whilst minimising the costs of investigation. This decision reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of patients, staff and the Company itself.

The Board of Directors of Directors recognises that the aim of IG forensics is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for formal dispute or legal process. In this context, IG forensics may include evidence in the form of log-files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that may be collected in advance of an event or dispute occurring.

The Board of Directors acknowledges that IG forensics provide a means to help prevent and manage the impact of important business risks. IG evidence can support a legal defence, it can verify and may show that due care was taken in a particular transaction or process, and may be important for internal disciplinary actions.

Definitions

Key definitions are:

- **IG Forensic readiness**

  The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.

- **IG Forensic readiness planning**

  Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence related monitoring and collection processes and capabilities, storage requirements and costs.

Policy objectives

The IG Forensics Policy has been created to:

- Protect the Company, its staff and its patients through the availability of reliable digital evidence gathered from its systems and processes;
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to Company business;
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required;
- Demonstrate due diligence and good governance of the Company's information assets;

Policy responsibilities

The Company Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of IG forensic policy procedures and standards for the Company.

The SIRO is responsible for the ongoing development and day-to-day management of the IG forensic policy within the Company's overall Risk Management Programme (Programme).

The Company Information Governance Lead (IG Lead) shall ensure that IG forensic readiness planning is adequately considered and documented for all information assets. Goals for IG forensic planning include:

- Ability to gather digital evidence without interfering with business processes;
- Prioritising digital evidence gathering to those processes that may significantly impact the Company, its staff and its patients;
- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to the Company;
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.

Forensic readiness plans shall include specific actions with expected completion dates.

The SIRO shall advise the Company Board of Directors on forensic readiness planning and provide periodic reports and briefings on progress.

Policy scope

This policy is applicable to all areas of the Company and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

Communication

This policy is to be made available to all Company staff and observed by all members of staff, both clinical and administrative.

There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.

SUBJECT ACCESS REQUEST POLICY & PROCEDURE

Introduction

Legislation provides that an individual has the right to request access to their personal information that is held by an organisation. The information can be health records, employment records, or records which hold information relating to them as the 'data subject'.

Southern Ultrasound must ensure that it has a policy in place (and supporting procedures) to respond to Subject Access Requests under the Data Protection Act 1998 and conforming to the strengthened rights provided with in the General Data Protection Regulations 2018 (GDPR).

As a general rule, Southern Ultrasound does not retain any patient identifiable information that therefore should never receive a Subject Access request, but it does hold non-clinical information on contacts for which the policy may be enforceable

Purpose & Scope

This policy deals with the rights of data subjects provided under Section 7 of the Data Protection Act whereby individuals can request access to their data. The Act gives individuals (known as data subjects) the right, subject to certain exceptions, to request access and obtain copies of personal data about themselves that is held in either computerised or manual formats and any type of personal information that is recorded including photographs, x-rays, audio messages and CCTV images.

Data subjects have access rights to their personal information irrespective of when the record was created. To exercise this right, an individual must make a written request for information. This is known as a subject access request.

A health record is defined as:

- Consists of information relating to the physical or mental health or condition of an individual and
- Has been made by or on behalf of a health professional in connection with the care of that individual

This policy applies to all staff employed by or working on behalf of **Southern Ultrasound** including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers or locums.

This policy applies to all requests for access to personal data held by **Southern Ultrasound**.

Policy Statement

This policy will provide a framework for **Southern Ultrasound** to ensure compliance with the Data Protection Act 1998. This policy is supported by operational procedures and activities connected with the implementation of Subject Access Requests, these are detailed in the document.

This policy matches the requirements identified by the Information Commissioner Subject Access Request Code of Practice August 2013 **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access**.

Principles

Individuals have the right to request copies of their information that the CCG may hold and to also request certain information relating to the processing of their information including:

- A description of the information
- The purposes the information is used for
- The disclosures that are made or might be made
- The source of the data

Southern Ultrasound is required to respond to Subject Access requests promptly within 40 calendar days of receipt of the request. Failure to do so is a breach of the Act and could lead to a complaint to the Information Commissioner (ICO). If it is anticipated that a request will take longer than the 40-day period, the Company must inform the applicant giving an explanation of the delay and agree a new deadline.

Failure to comply with a request for subject access, without valid justification, is treated as a serious matter and may be referred to the ICO. Such complaints are dealt with as a matter of priority and may lead to a full-scale investigation into an organisation's procedures and practices.

Who can make a request

Subject access requests can be made by:

- The individual themselves
- Individuals requesting access on behalf of a child for whom they have parental responsibility
- A representative nominated by the individual to act their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority
- In certain situations a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent

Individuals living abroad

Patients or individuals who used to live in the UK who have records held by **Southern Ultrasound** will still have the right to make a subject access request.

The same procedure would apply as for an individual living in the UK.

Roles & Responsibilities

Information Governance Lead (IG Lead)

The IG Lead is the accountable officer and Data Controller for **Southern Ultrasound**. The IG Lead is responsible for ensuring compliance with the Data Protection Act 1998.

Requests received by **Southern Ultrasound** staff will be forwarded to the IG Lead for review and response.

All request details will be entered into a log and this will be maintained to monitor compliance to ensure all requests are answered in a timely manner.

The IG Lead is then responsible for:

- Prior to the release of any information, the IG Lead must be satisfied as to the identity of the person making the request. **Southern Ultrasound** will not release any information until this identification has taken place.
- Providing advice to **Southern Ultrasound** staff on the withholding of certain information requested under the Data Protection Act.
- Liaising with other organisations if relevant to process the access request in the event of shared records/data

If an applicant is making a request on behalf of another, such as a relative or a child, then consent or valid authority or evidence of parental responsibility of the patient should be produced.

All Staff

All managers and staff will comply with any request for personal data forwarded by the IG Lead as quickly as possible, and will respond as soon as possible but before a deadline communicated by the IG Lead.

Subject Access Requests – the rights of individuals

The Data Protection Act 1998 ensures the transparency of data processing by obliging organisations to explain to individuals how their data is used (Principle 1) and by providing the right of subject access under Section 7.

Section 7 of the Act provides that individuals who request access to their data should:

- Be informed whether or not they are the subject of any data being processed by a data controller organisation; and
- Be provided with an understandable copy of the information held about them on request. It should also be provided in a 'permanent form' unless the provision of the information in a permanent form would involve 'disproportionate effort'. Individuals also have the right to:
    - A description of the personal data of which they are the data subject
    - A description of the purposes for which the data are being processed or are to be processed – this could be based on the information supplied to the Information Commissioners office during notification or on some information specific to the applicant;
    - Any information available to an organisation on the source of the applicant's data; and
    - Where the applicant specifically requests it, the logic involved in any fully automated decision-taking that has or may have a significant effect on the individual concerned, such as a decision in relation to risk stratification (except where the logic would constitute a trade secret or be regarded as commercially in confidence).

Consent Issues

In most cases the consent to access personal information will be provided by the individual who is requesting the information, however, there may be cases where the individual is unable to consent or the individual is a child.

When an applicant is not able to produce written consent from the patient to access the patient information or is not able to evidence that he/she is entitled to access the patient information, **Southern Ultrasound** will request further information from the applicant on the reason for the request to decide whether it would be justifiable to release the information to the applicant in any event.

In the event that the applicant is a solicitor the subject's written authority for release must be obtained.

Where a patient is unable to manage his/her own affairs then **Southern Ultrasound** will only accept an application by a person appointed by the Courts e.g. under the Court of Protection (or acting within the terms of a registered Lasting Power of Attorney - Health).

A young person over 16, but under 18, or a child under 16 who is considered to be Fraser competent may exercise their right of access to his/her health records under the Act (see Department of Health 'Best practice guidance for doctors and other health professionals on the provision of advice and treatment to young people under 16 on contraception, sexual and reproductive health' 2004). This is also in line with guidance issued by the Information Commissioner.

However, **Southern Ultrasound** must be particularly careful to verify that the young person has either initiated such a request or consented to such a request being made or that the young person's lack of understanding requires a parent or guardian to act on their behalf. Another important aspect may well be the nature of the personal information that will be supplied.

This will be of particular significance where the information may contain reference to the parent or guardian within the young person's records: for example, where allegations of abuse have been made against the parent or guardian in a social work file. **Southern Ultrasound** will need to handle requests from minors carefully; consideration needs to be given to balancing the harm that might arise against the possible benefits of supplying the information.

When an applicant is not able to produce a written consent from the patient to access the patient information or is not able to evidence that he/she is entitled to access the patient information, **Southern Ultrasound** will request further information from the applicant on the reason for the request to decide whether it would be justifiable to release the information to the applicant in any event.

Shared Records

There are situations where a subject access request involves a health record that is shared between healthcare organisations.

The modernisation and integration of health and social care will place a greater emphasis on shared records. In developing integrated health and social care service, **Southern Ultrasound** will set out its arrangements for managing the requirements of the Data Protection Act 1998 and Subject Access requests with its partners as part of any service reconfiguration or development.

The following principles will be followed where this is the case:

- Obligations under the Act are, in general placed on the holder of the record. If records are shared between two bodies, they will be joint data controllers. Responsibility for ownership of the record rests with the Secretary of State for Health although essentially, where both organisations are joint data controllers for the shared record, both are controlling how they are used
- In order to deal with Subject Access requests effectively, the organisation receiving the Subject Access request will take responsibility for processing the request and for obtaining consent or refusal for the release of parts of the record relating to the other organisation
- If **Southern Ultrasound** does not agree with the decision made by the other organisation to withhold data from release and subsequently releases that element of the record, it will accept full liability
- **Southern Ultrasound** must document the reasons for withholding certain information lawfully in the request log. The applicant may challenge the decision not to release information
- If there is a refusal to disclose the record from the partner organisation, the organisation dealing with the access request should, in their response to the applicant explain the reason for the refusal and refer them to the other partner organisation directly if they wish to contest the refusal.

Other Records

In addition to health records, all other records held by **Southern Ultrasound** containing individual's information are liable to subject access requests by those individuals or their representatives. This includes personnel, finance,

complaints and administration records. Any 'third party' content of the record must be referred to the originating organisation for consent to release.

Deceased Patient Records

The rights to access under the Data Protection Act 1998 extend only to living individuals. Requests for deceased patients' records are made under the Access to Health Records Act 1990. Requests can only be made by:

1. The patient's personal representative (usually the executor of the will or administrator of the estate) or
2. Any person who may have a claim arising out of the patient's death - release of any information will only be the minimum necessary to process their claim. Only relevant information relating to any claim made should be released

In order to show that the Applicant has been appointed as the personal representative **Southern Ultrasound** will ask for a copy of the Grant of Probate or Letters of Administration. **Southern Ultrasound** understands that these documents are not always available so will accept requests from the next of kin providing they have proof of identity and taking into account the patient's wishes before they died. **Southern Ultrasound** will also consider the confidentiality principles when releasing this information.

For more information please read 'Guidance for Access to Health Records Requests February 2010', which can be accessed on http://systems.hscic.gov.uk/infogov/links/dhaccessrecs.pdf.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice.

Record holders must satisfy themselves as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

A health professional must inspect records taking into account the following:

- If it is known whether the deceased patient did not wish for their records to be disclosed or the records contain information that the deceased patient expected to remain confidential
- If the release of the information is likely to cause serious harm to the physical or mental health of any individual

The same rules apply to third party information as with other health records. **Southern Ultrasound** should afford the same level of confidentiality to deceased patient's records as for living ones.

Exemptions to the Release of Information

The Data Protection Act 1998 makes provision for withholding information in certain circumstances which must be considered when a request is received.

If we believe that an exemption should be applied, legal advice will be required.

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 Creation:	18/09/ 2018 .	Date of Last review:	v.1 (N/A)
		Kevin Rendell	Director & IG Lead