Southend University Hospital NHS
NHS Foundation Trust

# Data Protection and Code of Confidentiality Policy

**SPONSOR (Information Asset Owner)**
Sue Hardy, Chief Nurse & Caldicott Guardian,

**AUTHOR (Information Asset Administrator)**
Dean Jones, Information Security Coordinator
Tracey Kalp, Information Governance Manager

**RATIFIED BY:**
Procedural Document Group

**APPROVED BY:**
Information Governance Committee

**TARGET AUDIENCE:**
All staff

**POLICY NUMBER:**
IS09

**POLICY CATEGORY:**
Information Security (IS)

**This document is available in large print and alternative formats. Should you or someone you know require this in an alternative format please contact us on 01702 435555 Ext. 6455 or e-mail nicky.frost@southend.nhs.uk**

| ISSUE AND REVISION RECORD: | | | |
|---|---|---|---|
| **Date** | **Issue No** | **Details** | **Review date** |
| 06/1998 | 01 | New document - Guidelines For Good Practice | 01/2000 |
| 10/2009 | 02 | Complete review and up graded to policy status | 10/2012 |
| 03/2011 | 03 | Reviewed and updated in line with version 8 of the IGT | 10/2012 |
| 10/2011 | 04 | Updated to appendix 5 | 10/2012 |
| 03/2013 | 05 | Reviewed updated in line with version 10 of the IGT | 03/2016 |
| 03/2014 | 06 | Reviewed and updated to include changes in governance team and national requirements/guidance. | 03/2016 |

# Contents

# 1 Introduction

Southend University Hospital NHS Foundation Trust is required to comply with legal obligations and NHS requirements relating to confidentiality and information security standards. The two key documents covering the security and confidentiality of Personal Confidential Data (PCD) processed within the NHS, UK and European Economic Area (EEA) are the Data Protection Act 1998 (DPA) and NHS Code of Practice: Confidentiality.

Southend University Hospital NHS Foundation Trust holds and processes information about its patients, staff and other individuals in order to carry out the business of healthcare provision. To comply with data protection requirements PCD must be collected and used fairly, stored securely and disclosed lawfully (See Appendix 1 for a summary of the DPA principles.)

Privacy Impact Assessments (PIA) are now mandatory for any new system (IT or otherwise), process or procedure that involves PCD. Southend University Hospital NHS Foundation Trust recognises the importance of innovation and change in business practices and will use PIAs to ensure the protection of PCD within its innovations.

The Trust also has a duty to comply with additional guidance issued by the Department of Health (DOH), Monitor and professional bodies, along with the legal requirements of the Common Law Duty of Confidence.

Legal requirements and NHS guidance apply equally to all forms of PCD, be it held manually or electronically. Failure of the Trust or its staff (including contractors and volunteers) to comply with legislation, in particular the DPA, will result in investigation and may risk the imposition of substantial fines by the Information Commissioners Office (ICO).

# 2 Purpose

The purpose of this policy is to:

- Give assurance to the Trust and individuals that PCD is dealt with legally, securely, effectively and efficiently, in order to maintain “excellent care by excellent people”.
- Bring to the attention of personnel, their responsibilities under the Data Protection Act 1998 and other related legislation and guidance, as part of the Trust’s Information Management framework.
- Ensure appropriate safeguarding and respect for the confidentiality of PCD.
- Ensure the Trust complies with data protection legislation, meets statutory obligations and observes standards of good information governance practice.
- Minimise the risks of information security breaches, prosecution and financial or reputational penalties.
- Enable information sharing when necessary in a responsible and lawful manner.

- Raise staff awareness about how to respond to requests for sharing confidential information.
- Ensure patients, carers and the public are provided with information about their rights under legislation.
- Provide direction to the advice, support and training available to all staff.

## 3 Definitions

| | |
|---|---|
| **Accountable Officer** | Should be Chief Executive; responsible for safeguarding public funds/assets, ensuring value for money, sound financial management systems in place and risk management systems. |
| **Anonymised Information** | Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. |
| **ABUD** | Associate Business Unit Director |
| **BMA** | British Medical Association |
| **BUD** | Business Unit Director |
| **Caldicott Guardian** | The term Caldicott derives from the 1997 report of the Review of Patient-Identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report). This review recommended establishing the role of the Caldicott Guardian to serve as the “conscience” of the organisation in relation to decisions about disclosure and to ensure senior level management of the confidentiality function which is itself a part of broader Information Governance. |
| **CCTV** | Closed Circuit Television – information recorded by video or other camera |
| **Data controllers** | The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed |
| **Data Flow** | An exercise to review and record where data is sent, what data has been sent and the purpose of sending that data |
| **Datix** | Trust risk register and incident reporting system. |
| **Disclosure** | This is the divulging or provision of access to data. |
| **DOH** | Department of Health |
| **DPA** | Data Protection Act 1998 – “The Act” |
| **EEA** | European Economic Area |
| **Healthcare Purposes** | These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities. |
| **Health and Social Care Information Centre (HSCIC)** | A national data, information and technology resource for health and social care. Playing a key role in driving better care, services and outcomes for patients. The trusted source of authoritative data and information relating to healthcare. |

| | |
|---|---|
| **Information Assets** | Any collection of information that is important to the Trust, e.g. database, case-notes |
| **Information Asset Register (IAR)** | A list of information assets, administrators, owners and risk assessments used by the Trust to understand and manage the asset risks to them. |
| **Information Asset Administrators (IAA)** | Information Asset Administrators are operational managers responsible for maintaining the integrity of one or more information asset, managing information risks locally and keeping an information asset register. The IAA is accountable to the IAO and the IAO to the SIRO in relation to maintaining confidentiality and security of the asset in compliance with Data Protection Act requirements |
| **IAO** | The role of Information Asset Owner was created following the Government's Review of Data Handling in Government (DHR) in June 2008, which also established mandatory minimum measures for personal data handling in Government. The IAO needs to manage information assets (within this person's remit of responsibility) so as to comply with statutory obligations (such as Freedom of Information, the Public Records Act and the Data Protection Act |
| **ICO** | Information Commissioner's Office |
| **Information Sharing Agreements (ISA)** | Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality, and data destruction between two or more organisations or agencies. |
| **Personnel** | All staff, managers and persons engaged in Trust activities that may have access to confidential information in particular sensitive and person identifiable information. This definition may include students, governors and contractors and persons working for the Trust on a voluntary non-remunerated basis. |
| **Personal data** | Personal data is anything which identifies an individual, either on its own or by reference to other information. |
| **Privacy Impact Assessment (PIA)** | Tool used to identify and reduce the privacy risks of new projects. It can help with the design of more efficient and effective processes for handling personal data. |
| **PCD** | Personal Confidential Information. |
| **Processing** | in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. |

| | |
|---|---|
| **Pseudonymised Information** | Like anonymised information, in the possession of the holder, an individual cannot be identified. However, the original provider of the information may retain a means of identifying individuals often being achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not. |
| **Safe Haven:** | The term **safe haven** is term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles. |
| **Sensitive personal data** | The DPA recognises that some types of personal information are more sensitive than others and imposes additional requirements for processing sensitive personal data. |
| **Statement of Internal Control (SIC)** | Public accountability document that describes the effectiveness of internal controls in an organisation and is signed by the Accountable Officer. |
| **SIRO** | Senior Information Risk Owner is the Trust's Chief Operating Officer. The SIRO acts as an advocate for information risk on the Board and in internal discussions. |

# 4 Duties

## 4.1 Duties within the Trust (Committees)

**The Information Governance Committee** - is chaired by the Trust SIRO and is responsible for:

- Approving, as required, compliance management arrangements (including PIAs) before the introduction of new information processes.
- Approving, as required, new IT system specifications with regard to information management arrangements (including PIAs when appropriate).
- Standardising and approving a consistent approach to obtaining consent to disclosure of information.
- Reviewing action plans related to the management of information security breaches/incidents.
- Providing a focal point for the resolution and/or discussion of information governance issues, ensuring the communication to all staff of lessons learned and changes in practice.

**The Audit Committee** – is responsible for:

- Receiving matters of escalation from the Information Governance Committee for discussion or action.
- Reviewing internal audit recommendations and monitoring progress against associated action plans.
- Approving the Information Governance report for publication.

### 4.2 Duties of Individuals within the Trust

**The Chief Executive -** as the Trust's Accountable Officer has ultimate responsibility for compliance with the Data Protection Act, ensuring:

- Responsibility for bringing data protection act issues to the attention of senior level managers is delegated appropriately to a Director or equivalent;
- The roles of Caldicott Guardian and Senior Information Risk Owner (SIRO) are appropriately assigned and supported;
- The annual Information Governance Toolkit submission is submitted and signed off and includes an appropriate assurance statement.

**Senior Information Risk Owner (SIRO)** – Board appointed executive director responsible for ensuring:

- Serious data protection issues are brought to the Board for discussion as required;
- A lead or manager is in place to organise and enforce the Trust's approach to data protection;
- Written advice is provided to the Accountable Officer and Trust Board regarding the information risk/security content of the annual Statement of Internal Control (SIC) and annual report.
- As chairman of the Information Governance Committee, that meetings are appropriately attended.

**Caldicott Guardian** – Board appointed clinical executive director responsible for:

- Protecting the confidentiality of PCD processed by the Trust, ensuring that SUHFT and partner agencies satisfy the highest practical standards for handling PCD.
- Acting as the "conscience" of the Trust, by actively supporting work to enable information sharing where this is appropriate and advising on lawful and ethical solutions.
- Reviewing and authorising, where appropriate, information sharing agreements and requests for disclosure of PCD.
- Championing confidentiality and information sharing requirements and issues at Board level and, where appropriate, at a range of levels within the Trust's overall governance framework.

**Associate Director for Governance** - supports the Caldicott Guardian and SIRO functions, and is responsible for:

- Overseeing the organisation and implementation of the Trust's information governance work programme (including DPA and Caldicott work plans).
- Managing the confidentiality and data protection components of the information governance toolkit, contributing to the annual assessment.
- Supporting the roll out of information governance training (including data protection and Caldicott awareness).
- Ensuring, along with the SIRO, Information Security Co-Ordinator and Information Governance Co-Ordinator, that Information Asset Owners (IAOs) are nominated to manage local responsibilities under DPA and confidentiality within their work area.

**Information Security Co-Ordinator and Information Governance Co-Ordinator** – as key members of the Trust's information governance team are responsible for:

- Undertaking the annual Data Protection census and collating assurance evidence supporting the submission of the Information Governance Toolkit year-end report by the Chief Executive ;
- Advising where changes are required to the Trust's Data Protection Registration status and maintaining this registration;
- Maintaining the currency of the Trust's Data flow maps and Information Asset Register (IAR)
- Providing advice and support concerning the management of data protection issues and any information security breaches;
- Managing, with others, fulfilment of the Trust's external reporting requirements;
- Maintaining the Caldicott Guardian disclosure log;
- Advising on, and maintaining the currency of the Trust's Information Sharing Agreements (ISA).
- Reviewing and revising this policy as necessary;
- Co-ordinating the work of others with data protection responsibilities;
- Supporting investigations into confidentiality breaches or potential breaches with relevant IAOs/IAAs; ensuring reports and action plans are presented to the Information Governance Committee for monitoring of completion.
- Working with the Trust's Freedom of Information Act Co-ordinator to ensure adherence to data protection requirements;
- Liaising with the Trust's training and development team to provide information governance training (including data protection and caldicott responsibilities), through induction and on-going face to face or e-learning courses.
- Assist in the administration of the information governance training tool database.
- Complete new and review on-going information governance risk assessments recorded on the Trust's risk register so as to ensure business continuity.
- Support the communication of key risk management and other information governance material to all staff to assist the achievement of best practice.
- Provide monthly reports to the Information Governance Committee on caldicott and data protection matters.

**Information Asset Owners (IAO's)** – usually the BUD or ABUD and are responsible for:

- Working with the information governance team and other IAOs to ensure a clear understanding of responsibilities and accountabilities relating to asset ownership. Especially vital where information assets are shared by multiple parts of the Trust.
- Supporting the SIRO in the overall information risk management function.
- Ensuring actual or potential breaches of confidential are reported on DATIX and investigated to ensure lessons are learned and necessary changes in practice are made (in line with the Trust's incident reporting policy).

**Information Asset Administrators (IAA's)** – generally system managers and are responsible for:

- Undertaking reviews/follow up of failed log-in reports provided for systems for which they are responsible; reporting results to the Information Security Co-Ordinator and Information Governance Committee, as required.
- Ensuring security risks are controlled, risk assessments are in place detailing control measures and that these are regularly reviewed.

**Departmental Managers** - are responsible for informing the information governance team of any new uses of Personal Confidential Data (PCD) within their area of responsibility; to assist in the statutory requirement to keep the Trust's Data Protection registration up to date.

**All Staff (including contractors and volunteers)** – are subject to an obligation of confidentiality and must adhere to the Data Protection Act, Caldicott guidelines, professional codes of conduct and responsible for:

- Undertaking training as identified by their line managers as required for their role.
- Ensuring they are adequately trained and aware of their personal responsibilities for data protection and confidentiality.
- Knowing how to avoid information security breaches.
- Knowing how to obtain support and advice concerning disclosure requests.
- Ensuring they are aware of the process for reporting all incidents where security of PCD has been breached.

# 5 Data Protection Act 1998

The Data Protection Act 1998 lays down regulation for the handling of personal data. For such data it is essential to abide by the 8 principles (see Appendix 1). The Act also sets out that information must only be disclosed on a need to know basis.

It can be difficult to comply with the Act, as it is not always clear what actions need to be taken. The Trust needs it staff to safeguard the balance between the perceived need for information and the individual's right to respect for their private life.

The following checklist has been compiled by the ICO to help comply with the Act:

- Do I really need this information about the individual?
- Do I know what I am going to use it for?
- Do the people I hold information about know that I hold it, and are they likely to understand what it will be used for?
- If I am asked to pass on personal information, would the people about whom the information is about expect me to do this?
- Am I satisfied the information is being securely held, either on paper or computer?
- Is our website secure?
- Is access to personal information limited to those with a strict need to know basis?
- Am I sure the personal data is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?

Under the Data Protection Act 1998, before personal data can be held on computer, it is necessary to notify the Information Commissioner's Office. Therefore, all IT applications/databases containing Personal Confidential Data (PCD) will be registered under the Southend University Hospital NHS Foundation Trust's global notification (Z1972899)

# 6 Caldicott Role and Responsibilities

The term Caldicott is derived from the 1997 Caldicott Committee report, which then led to the publication of Confidentiality: NHS Code of Practice. This mandated that each NHS organisation is required to have a Caldicott Guardian, to serve as the "conscience" of the organisation in relation to decisions about disclosure and ensure senior management of confidentiality matters.

All NHS Trusts are required to maintain and update their Caldicott Guardian registration managed by the Health and Social Care Information Centre (HSCIC). For Southend University Hospital NHS Foundation Trust this function is carried out by the information governance team.

The Caldicott principles were recommended by the Caldicott Committee as a guide for the NHS for the use and transfer of PCD. In April 2013, the results of a further information review lead by Dame Fiona Caldicott were published. The recommendation reinforced the six original Caldicott principles and made one addition.

The seven principles provided by the 2013 report are the baseline for good practice;

- **Principle 1** – Justify the purpose(s) for using confidential information.
- **Principle 2** – Only use it when 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** – Duty to share information can be as important as the duty to protect patient confidentiality.

Individuals who believe that they have suffered damage as a result of misuse of their personal data may make a claim for compensation against the Trust, and against any negligent employee. Additionally, since April 2010, the ICO can fine the Trust up to £500,000 as a penalty for serious breaches of the Data Protection Act.

In supporting fair, lawful and justifiable decisions to safeguard against harm to individuals or the Trust's reputation; the Caldicott Guardian requires the support of all staff. Staff must be willing and able to access advice, as well as understand and adhere to, the Data Protection Act and other legal requirements including the Trust's Code of Confidentiality (Appendix 2).

## 7. Senior Information Risk Owner (SIRO)

The establishment of the role of SIRO is one measure introduced to strengthen controls around information security. The SIRO should be an executive on the Board who is familiar with information risks and the organisation's response to risk; and has the knowledge/skills necessary to provide the required input and support to the Board and Accountable Officer.

## 8. NHS Care Record Guarantee and NHS Constitution

The NHS Constitution and NHS Care Record Guarantee set out the commitment for confidentiality that patients/public can expect from NHS organisations.

- We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does.
- We will take appropriate steps to make sure we hold records about you, both paper and electronic, securely and only make them available to people who have a right to see them.
- We will take action when someone has deliberately accessed records about you without permission or good reason. This can include disciplinary action, ending a contract, firing an employee or bringing criminal charges. We will tell you if that happens.

The Trust will ensure all staff are aware of these commitments by making annual information governance training mandatory for all staff. Southend University Hospital NHS Foundation Trust will also raise awareness of responsibilities to safeguard the confidentiality of PCD through departmental spot checks, face-to-face advice and training, and through staff communications.

## 9. Protecting Personal Confidential Data (PCD)

### 9.1 Securing your area of work

- Administrative rooms/areas should be sited in such a way that only authorised staff can enter i.e. the area is not readily accessible to all members of staff working in the building, or to visitors.
- Ground floor administration rooms should have locks on all windows.
- Rooms/areas should conform to health and safety requirements in terms of fire, flood, theft or environmental damage.
- Manual paper records containing PCD should be stored in locked cabinets when not in use.
- Computers should not be left on view, or accessible to unauthorised staff; must have a screensaver function and be locked or switched off when not in use.
- Computer screens must be facing away from public areas, wherever practical.
- Equipment such as fax machines must be kept in a locked office, have a coded password and be turned off out of office hours (where practical).
- Printed information containing PCD must not be put on display in public areas e.g. test results, theatre lists on walls/windowsills of wards or clinics.
- Whiteboards in public areas must not show the key to information put on them.

### 9.2 Unauthorised Access

- Information held by Southend University Hospital NHS Foundation Trust will only be accessed by authorised staff as required to carry out the course of their duties.

- Staff will only access the minimum information necessary for patient management, care and to carry out their Trust duties.

- Staff will not look up or access information relating to themselves, family members, other relatives, friends, neighbours, public figures/celebrities or patients not under their care.

## 10. Safe Transfer of Information

### 10.1 Communication by Post

- Paper communication containing PCD must be transferred in a sealed envelope and addressed by name to the recipient. They must be clearly marked “Personal and Confidential – To be opened by recipient only”.
- When using window envelopes, ensure that only the name and address are visible.
- Checks must always be made to ensure the information is being sent to the correct person.
- An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.
- PCD contained in paper transfers must be limited to those details necessary for the recipient to carry out their role.

### 10.2 Communication by e-mail

- Unencrypted transfer of personal information by e-mail to patients is allowable with the informed consent of the data subject/patient. Informed consent must be recorded in the medical record.

- If there is a need to send PCD to other organisations for healthcare purposes on a regular basis, this must be done through the Trust's secure e-mail (access via completion of the form on StaffNet, see Appendix 3). Alternatively, through NHS Mail (the only BMA/DOH approved for secure exchange of PCD across NHS organisations).
- Requests for secure e-mail access must be approved by a line manager and sent by e-mail via the IT helpdesk to the Information Security Co-Ordinator for authorisation.

### 10.3 Verbal Communication

- Care must be taken to ensure personal details are not overheard by staff/public/relatives who do not have a "need to know". Wherever possible, discussions should be held in private locations and not in public areas, staff common areas or lifts.
- If information must be shared by telephone, steps must be taken to ensure the recipient is properly identified. This can be done by taking a phone number, double-checking that it is the correct number for the individual/organisation. Checking the individual/organisation has a legitimate right to the information i.e. Next of Kin, part of the multidisciplinary care team, then call them back.
- Messages containing PCD must not be left on answer machines, unless a password is required to access them. They should never be left on communal systems.

### 10.4 Communication by Fax

- Fax machines are one of the most common causes of confidentiality breaches, many are used by several different departments and people often collect faxes without checking all pages are for them; increasing risks of information being seen by unauthorised persons. Therefore, fax transmission should be avoided wherever possible.
- Where it is necessary to fax PCD to another organisation this should be done in the first instance to a Safe Haven fax machine; this will be located in a secure area and designated to receive confidential information.
- If the recipient does not have a Safe Haven fax machine available, the following rules must be followed:
    - Telephone the recipient of the fax and inform them that you will be sending confidential information by fax.
    - Check the fax number with the recipient and ask them to wait by that fax machine whilst the information is sent.
    - Make sure the fax cover sheet states that the information is confidential.
    - Pre-programme numbers for regular recipients into the fax machine where possible and double check the number dialled/selected is correct before sending the document.
    - Request a report sheet to confirm successful transmission and call back the recipient to confirm successful receipt.
- Staff must never:
    - Send faxes if you know the information will not be seen/picked up for a period of time.
    - Send faxes at times outside of the recipient's hours of work.

- Leave information unattended whilst a fax is being sent or received. This is particularly important if the receiving fax machine is engaged/unavailable.

### 10.5 Transporting Paper PCD around Trust Sites

- Many unauthorised breaches of PCD are caused by staff leaving papers in areas around the Trust e.g. toilets, dining rooms, library or dropping them en-route.
- Take care to keep papers on you at all times if you have to carry documents containing PCD and pick them up when you leave an area.
- Wherever possible, carry them in a folder or envelope to prevent the information being seen.
- Ensure the documents are appropriately filed or confidentially disposed of when no longer required.

### 10.6 Transporting PCD off Trust Sites

- Use of encrypted data off site must be formally authorised. Applications should be made by completing the Removable Media Authorisation form found on the Trust's StaffNet site.
- Permission to take paper records or other un-encrypted data off site must be applied for by completing the "Off-site Unencrypted Personal Data User Authorisation Form found on the Trust's StaffNet site.
- On completion the form must be sent to the Information Security Co-Ordinator/Information Governance Co-Ordinator, who will review and ensure authorisation where appropriate, from the Caldicott Guardian. All requests and decisions will be logged on the Trust's Caldicott log.

### 10.7 Transfers of Personal Confidential Data Abroad

- Principle 8 of the Data Protection Act 1998, governs transfers of personal data and requires that it is not transferred to countries outside the European Economic Area (EEA), unless that country has adequate level of protection for information and the rights of individuals.
- The information security co-ordinator and information governance co-ordinator **must** be consulted where the transfer of PCD to countries outside the EEA is being considered/requested. Final approval for such transfers will be only be given by the Caldicott Guardian or authorised deputy, and in line with ICO best practice guidance.

### 10.8 Use of Social Media

- Southend University Hospital NHS Foundation Trust recognises that many staff share professional knowledge and experience with other professionals and acknowledges that staff can benefit in professional development through relevant social media. Nevertheless, the Trust has an obligation to protect its information assets and patients' privacy, and so has restricted access from Trust resources to a limited number of social network sites (see Appendix 4).

- Official Trust blogs and websites are managed by the Trust's corporate communications team and staff contributing to or maintaining these are guided by their local operating procedures. Staff outside the communications team are not authorised to communicate by any means on behalf of Southend University Hospital NHS Foundation Trust, unless approved in advance.

- Staff are ultimately responsible for their own online behaviour, but are advised not to divulge details of their employer within their personal profile page (i.e. in accordance with professional guidelines such as “RCN Legal Advice on Using the Internet”. Staff who do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.

- Staff must avoid online statements, posts or actions that are inaccurate, libellous, defamatory, harassment, threatening or may otherwise be illegal or bring the Trust reputation into disrepute.

- Staff using social media privately, must not disclose Southend University Hospital NHS Foundation Trust information that is, or may be, sensitive/confidential, or that is subject to a non-disclosure contract. This includes information (written or photographic) about patients, colleagues, contractors, other organisations, commercial suppliers or Trust business activities.

- Breaches will be investigated and result in disciplinary actions in accordance with Trust policies and procedures, and has the potential to lead to civil or criminal proceedings against individuals.

## 11. Disclosure of PCD

- Patient’s retain the right to restrict disclosure of their personal information to other healthcare professionals or to relatives or carers. In these circumstances, patients should be encouraged to be very explicit abut persons they do not want to access their information. In all cases the wishes of the patient must be accurately recorded in their medical records.
- There are occasions when Southend University Hospital NHS Foundation Trust, will be bound to disclose confidential information but without consent for the following:
    - Birth and death notifications
    - Notifiable communicable diseases
    - Poisonings and serious accidents in the workplace
    - Terminations
    - Misuse of drugs
    - Safeguarding children and vulnerable adults
    - Road traffic accidents
    - Prevention / detection of a serious crime i.e. murder or terrorism.
- There are also rare occasions where a patient’s confidentiality may be overridden and this decision must only be made by the senior clinician involved at the time. Examples of these circumstances include:
    - Where the patient’s life may be in danger, or where the patient may not be capable of making an informed decision.
    - Where there is serious danger to other people, where the rights of others may supersede those of the patient.
    - Where there is a serious threat to the healthcare professional.
    - Where there is a serious threat to the community

- PCD can also be requested for disclosure by the Police, Social and Probation Services, under section 29(3) of the Data Protection Act 1998: Crime, Taxation and Fraud.
- Disclosures may also be permitted, subject to application and approval, under Section 251 of the NHS Act 2006.
- Decisions regarding disclosure of confidential information by Southend University Hospital NHS Foundation Trust without the individuals consent must be taken by the Caldicott Guardian, or nominated deputy, and recorded on the Trust's Caldicott log.
- Where there is a need to disclose PCD the Disclosure Form (Appendix 5) must be completed and sent to the information governance team (Information.Governance@southend.nhs.uk) who will ensure all the information is fully completed prior to Caldicott Guardian review.

## 12. Processing and Sharing Information to Support Healthcare

### 12.1 Third Party Contractors

- Third parties may be granted access to Trust information in a number of ways, and it is vital that the nature and level of access is risk assessed before confidentiality elements of contracts are drawn up.
- Third party access may be granted to Trust systems and networks e.g. clinical system software may be maintained by the system suppliers under contract. In these cases it is most likely that the suppliers' staff may have substantial access to confidential data. Confidentiality and non-disclosure clauses must be included in the contract between the Trust and system supplier.
- As part of the procurement process the Trust information governance team will also investigate security controls in place with third party suppliers; including:
    - Are there adequate security controls, policies and training?
    - Are staff screened prior to employment?
    - Are they registered for data protection with the ICO?

### 12.2 Information Sharing Agreements (ISAs)

- Information Sharing Agreements(ISA) are required for Southend University Hospital NHS Foundation Trust to manage and record the use and transfer of PCD with partner agencies for purposes other than direct continuing clinical care.
- These documents set out the requirements for all signatory organisations in order to carry out responsible information sharing and cover:
    - Who the partners to the agreement are
    - What information is to be shared
    - What powers in law enable the ability to share information
    - How the information is to be shared
    - Necessary security arrangements
- Staff must contact the Information Security Co-Ordinator or Information Governance Co-Ordinator if an ISA is required, as the documents must be approved by the Caldicott Guardian for each partner organisation.

### 12.3 Use of PCD for Clinical Training

- Use of patient information is essential to the education and training of healthcare professionals. For the majority of uses anonymised information is sufficient and must be used whenever practical.
- Where trainee clinicians are part of the team providing a patient's care they can access the relevant PCD with the patient's consent. The lead clinician has responsibility for obtaining this and recording within the medical record.
- Trust staff must request and document patients' informed consent prior to making any audio or usual recordings for training purposes.

## 13. Confidentiality and Data Protection Compliance of New Processes

- Innovations in healthcare are likely to have an impact on the Trust's processes and systems. In order to comply with statutory requirements it is vitally important that new processes maintain the confidentiality, integrity and accessibility of information.
- The information governance department must be informed of all new proposals to the Trust. This is to ensure that the appropriate Privacy Impact Assessment (PIA) is carried out and information risks considered within early stages of project management.
- Concerns or issues relating to the information governance of a new process will be taken to the Information Governance Committee via a member of the information governance team.
- ICO advice states that the use of PCD for IT system testing should be avoided. Where there is no practical alternative to using live data, IT department staff and system suppliers should develop alternative methods of system testing.

## 14. Information Governance Training

All staff employed by the Trust, who provide a service to the Trust under contracts or as volunteers, must take and pass annual information governance training. The Trust has also developed in information handbook which gives practical guidance on keeping PCD safe and on legal disclosure.

## 15. Monitoring Compliance

| Aspect of compliance or effectiveness being monitored | Monitoring Method | Individual department responsible for the monitoring | Frequency of the monitoring activity | Group/Committee/forum which will receive the findings/monitoring report | Committee/individual responsible for ensuring the actions are completed |
|---|---|---|---|---|---|
| Keeping PII confidential | Area audits and questions to staff. | Information Security Coordinator | Ad-hoc covering all areas in the year | Information Governance Committee | Business Unit Governance Leads / Directors |
| Reporting data confidentiality incidents | Reporting breach of confidentiality incidents | Information Security Coordinator | Monthly | Information Governance Committee | Business Unit Governance Leads / Directors |

| | | | | | |
|---|---|---|---|---|---|
| Caldicott Log-disclosures/ | Logging and reporting | Governance Manager | Monthly summary | Information Governance Committee | Information Governance Committee |
| IG training figures | Monitoring | Information Security Coordinator | Monthly actual against target | Information Governance Committee | Business Unit Governance Leads / Directors |

## 10 Associated Documents

This policy should be read in conjunction with the following documents:

- IS01 Information Security Policy
- IS07 Acceptable email usage policy
- IS21 Access Control Policy
- IS26 Policy for the Management of Data Quality
- IS30 IT Security Policy
- IS37 Mobile Devices Policy
- IS38 Registration Authority Policy
- IS39 Internet Acceptable Usage Policy
- IS41 Pseudonymisation and De-Identification Policy
- IS43 Bring Your Own Device Policy
- RM10 Incident and Near Miss Reporting Policy and Procedures
- RM12 Assurance Framework Risk Management Strategy
- CM06 Policy for Consent to Treatment or Examination
- CM10 Complaints Policy and Procedure
- CM17 Procurement Strategy & Policy
- CM38 Records Management Strategy
- Trust's Information Governance Handbook

## 11 Equality Impact Assessment

This policy has been the subject of an Equality Impact Assessment. The output of the assessment demonstrates that no one as a consequence of this policy is placed at a disadvantaged over others.

## 12 References

NHS Constitution
Confidentiality : NHS of Practice (PDF, 220K)
NHS Connecting for Health: *Health & Social Care Members: What you should know about Information Governance*
*Confidentiality: NHS Code of Practice. Supplementary Guidance: Public Interest Disclosures*
The Health Service Ombudsman: *Sharing and Publishing Information about NHS Complaints*,
The NHS Care Record Guarantee for England
The International Information Security Standard ISO/IEC 27002:2005
The Information Security Code of Practice
The Records Management NHS Code of Practice

Care Quality Commission: The Right Information in the Right place at the Right time
Research Governance Framework
NHS Information Risk Management :Digital Information Policy NHS Connecting for Health January 2009
Caldicott Guardian Manual
ICO's CCTV revised code of Practice

ICO's Data Sharing Code Practice and Data Sharing Checklist

NHS Information Governance: Information Risk Management Guidance: Fax Printer Ribbon and Film

HM Government Information Sharing: Guidance for Practitioners and Managers
Endorsing and supportive statements
Information Commissioner's Guidance on data security breach management
Department of Health : Checklist for Reporting, Managing and Investigating
Information Governance Serious Untoward Incidents Gateway Ref: 13177

Information Commissioner: Data Protection Audit Manual

Information Commissioner: Anonymisation: Managing data protection risk code of practice

Information Commissioner: Bring Your Own Device Guidance

Information Commissioner: IT Asset Disposal for Organisations Guidance
Information Commissioner: Conducting Privacy Impact Assessments Code of Practice

Information Commissioner: Privacy Notices Code of Practice

Information to share or not to share: The Information Governance Review

DOH, Information to share or not to share: The Government Response to the Caldicott Review

## APPENDIX 1 The Eight Data Protection Act 1998 Principles

| | |
|---|---|
| **1. Processed fairly and lawfully** | In practice, this is the most important principle. To comply, processing must be justified under one of several conditions set out in the Act. The most important condition is that the person has given his / her consent. Where the data is "sensitive", consent must be "explicit". Also, under this principle, a person must be fully aware of the ways in which their personal data may be processed in order for that processing to be considered fair. |
| **2. Processed for limited purposes** | Data may only be used for the purposes for which it was collected and not for other purposes. |
| **3. Adequate, relevant and not excessive** | Only information needed should be collected. For example, applicants for jobs should not be asked to provide information which, in fact, will only be needed for the successful candidate. |
| **4. Accurate and up to date** | Reasonable steps need to be taken to ensure the accuracy of information. This could include periodically checking that data held remains accurate and up-to-date. |
| **5. Not kept for longer than is necessary** | Personal data should not be kept for longer than is necessary. Equally, it should not be discarded if doing so would render the record inadequate. Specific legal provisions may require the retention of records for a set period (for example, tax/compliance records). It may be necessary in some cases to retain information to defend legal claims which may be made in the future. Unless there is some legitimate reason for keeping them, personal data should be deleted. |
| **6 Processed in line with individuals' rights** | Individuals have a right to see information that is held about them. This is known as the right of "subject access".<br>A subject access request must be dealt with promptly and in any case within 40 days of the date of receiving it.<br>Not all information should be disclosed. For example, information about other people or which was received in confidence should not be disclosed. |
| **7 Data security** | This principle requires that appropriate policies and procedures are in place to safeguard personal data. This includes implementing a data security policy; restricting access to data to authorized personnel; making sure that data is physically secure; training and educating staff about security measures; ensuring IT systems can withstand unauthorized access.<br>It also means ensuring that a contract is in place with any service provider appointed to carry out any data processing services, which includes clauses giving appropriate guarantees regarding data security. |
| **8 Not transferred to other countries outside the EEA without adequate protection** | Transferring personal data outside the EEA without taking adequate legal precautions is a serious breach as it effectively means that data subjects lose the protection of the Act. There are a range of options as to how to carry out international data transfers legally. |

# APPENDIX 2. SUHFT Code of Confidentiality

## What is confidential patient information?

1. 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. must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

2. Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. What this entails is described in more detail in subsequent sections of this document, but a key guiding principle is that a patient's health records are made by the health service to support that patient's healthcare.

3. One consequence of this is that information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

## Disclosing and using confidential patient information

1. It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies. Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule, described later in this document, but it applies in most circumstances.

2. Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways.

## Patient consent to disclosing

1. Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

2. Where patients have been informed of:

    a. the use and disclosure of their information associated with their healthcare; and
    b. the choices that they have and the implications of choosing to limit how information may be used or shared; then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent.

3. Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

4. There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Applications, and approvals, made under section 251 of the NHS Act 2006 (formerly section 60 of the Health and Social Care Act 2001) may support a range of important work such as clinical audit, record validation and research. Approved applications can be used to support disclosure without the consent of patients.

## Obligations on individuals working in the NHS

1. All staff should meet the standards outlined in this document, as well as their terms of employment (or other engagement agreements). Much of what is required builds on existing best practice. What is needed is to make this explicit and to ensure that everyone strives to meet these standards and improves practice.

2. Clearly staff are constrained from meeting these standards where appropriate organisational systems and processes are not yet in place. In these circumstances the test must be whether they are working within the spirit of this code of practice and are making every reasonable effort to comply.

## Contact information

For further help or guidance please contact the Information Security Co-ordinator on 8188 in the first instance.

## APPENDIX 3 Secure E-mail Messaging form

### Secure External E-Mail Messaging Request Form

In order to comply with the Data Protection Act 1998, Trust Information Security Policy and other relevant legislation and NHS guidance, this form will need to be completed for requesting the ability to send Person Identifiable Information (PII) securely from the Trust via e-mail.

| **PERSONAL INFORMATION** | |
|---|---|
| User Name: | Department: |
| Job Title: | Contact Number: |
| **Purpose of Use** | |
| Please give justified business purpose for the need to send PII via e-mail: | |
| **External Recipient Locations** | |
| Please detail locations that secure PII e-mail could be sent to (e.g. NHS South East Essex): | |
| **Approval by Senior Manager** | |
| I consider it necessary for the above name individual to be allowed to send PII securely out of the Trust by e-mail. I undertake to ensure that he/she is fully aware of the additional responsibilities under the Trust's Information Security Policy. | |
| Managers Name: | Department: |
| Job Title: | Internal Phone No: |

# APPENDIX 4 Approved Social Media Sites

## All Staff

- LinkedIn
- Twitter

## Corporate Communications

- Facebook

# APPENDIX 5 Request for disclosure of PII

## REQUEST FOR DISCLOSURE OF PERSONAL DATA

**Our Reference:** …….…… **Date:** …….
**To** (Authority): …Southend University Hospital Foundation Trust …….
**From (Officer)** ……**Designation:** ……
**Organisation:** ……**Address**……..……...
……...
**Fax No:** …… ……..

---

**Name**: ……. Male/Female **DOB:** ……. **Age:** ……

**Racial Origin** (please circle):

White British/White Irish / White European/ White Other/ Black Caribbean / White & Black African / White & Asian /Other Mixed/ Indian / Pakistani / Bangladeshi / Other Asian /Black Caribbean/Black African/Other Black/Chinese / Other ethnic group / Ethnic origin unknown

---

**Information Required**

Please tick relevant category and provide details of the purpose for which the data is to be used:

| | | |
|---|---|---|
| **Prevent crime** | | |
| **Detect crime** | | |
| **Prevent disorder** | | |
| **Detect disorder** | | |
| **Prevent nuisance** | | |
| **Prevent annoyance** | | |
| **Other (please describe)** | | **Signed:** ……..…… |

---

**Information supplied:** Yes/No* (please delete)

**If YES** summary of information supplied: ……..……

email detailing the investigations undertaken in respect of allegation made

……

**Can innocent victim, witness or person other than the person named above be identified if this information is disclosed?**

**If NO** why was information not supplied: ……..……

……

**Signed: ……**

**The use of this information for any secondary purpose is prohibited without the consent of the Data Holding Authority and/or the consent of the data subject**