Data Protection, Caldicott & Confidentiality Policy

Purpose of Agreement	This document describes Solent NHS Trust's policy on Data Protection, Confidentiality and Caldicott Guidance, and employees' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and on computers.
Document Type	[x] Policy [ ] SOP [ ] Guideline
Reference Number	SolentNHST/Policy/IG/02
Version	4
Name of Approving Committees/Groups	ICT Group Policy Steering Group
Operational Date	March 2018
Document Review Date	March 2021
Document Sponsors (Name & Job Title)	Chief Medical Officer and Caldicott Guardian Chief Operating Officer and SIRO
Document Manager (Name & Job Title)	Data Protection Officer and Head of Information Governance Security
Document developed in consultation with	ICT Group Policy Steering Group
Intranet Location	Policies and Procedures – Solent
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Data Protection, Caldicott & Confidentiality Policy & Procedures, Data Protection, Caldicott, Confidentiality, Safehaven

Amendments Summary:

Amend No	Issued	Page	Subject	Action Date
		Appendix E	Public Interest Disclosures	November 2010
		Appendix F	IG Risk Assessment	November 2010
		Various	Minor amendments/ updates throughout policy	November 2010
1	Feb '12		Name & Logo Change	Feb 2012
2	Feb '12	26	Data Flow Mapping	Feb 2012
3	January 2015	12	Addition of new Caldicott Guardian Principle	January 2015
3	January 2018	14 15 16	Addition of; 5.3 Breach of Confidentiality 5.4 PID in Medical Research 6 Privacy Impact Assessments 7.4 Data Protection Officer Role	January 2018

Review Log

Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
Prior to October 2010			Solent NHS Trust was established on 1st April 2010 through the integration of Southampton Community Healthcare (West) and Portsmouth Community & Mental Health Services (East).	Refer to; • NHS Southampton City's Data Protection, Caldicott & Confidentiality Policy
V1	Feb 12	Head of Information Governance	NHSLA Policy Committee Information Governance Steering sub-Committee	No changes
V2	Jan 13	Information Governance Manager	NHSLA Policy Committee Information Governance Steering sub-Committee	Text message review in line with Information Security Policy
V3	January 15	Information Governance Manager	NHSLA Policy Committee Information Governance Steering sub-Committee	Addition of new Caldicott Guardian Principle General Review
V4	November	Data	ICT Group	Minor admentments

	2017	Protection Officer and Head of Information Governance Security	Policy Steering Group	Additions made (see Amendments log above)

Table of Contents

1 Introduction & Purpose

1.1 Legislation:

1.1.1 Solent NHS Trust has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by NHS Digital, the Information Commissioners Officer, other advisory groups to the NHS and guidance issued by professional bodies.

1.1.2 All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the organisation. Penalties could be imposed upon the organisation and/or its employees for non-compliance with relevant legislation and NHS guidance.

1.1.3 Solent NHS Trust holds and manages a great deal of personal and confidential information relating to patients, service users and carers, the public and employees of the NHS.

1.1.4 The **Data Protection Act 1998** (DPA 98) provides controls on the handling of personal identifiable information for all **living** individuals. Central to the Act is compliance with the eight data protection principles (see 3.1) designed to protect the rights of individuals about whom personal data is processed whether an electronic or a paper record.

1.1.5 The **Access to Health Records Act 1990** provides controls on the management and disclosure of health records for **deceased** patients. Thus the personal representative of the deceased or a person who might have a claim arising from the patient's death can apply to request access to the files.

1.1.6 The **Caldicott Reports** provide guidance to the NHS on the use and protection of patient identifiable data (PID), and emphasises the need for controls over the availability of such information and access to it. It makes a series of recommendations and identifies that all NHS organisations are to ensure that they have an appointed Caldicott Guardian who is responsible for compliance with the Caldicott Principles and Standards, (see 3.2)

1.1.7 The **Common Law Duty of Confidentiality** prohibits use and disclosure of information, provided in confidence unless there is a statutory requirement or court order to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect the vital interests of the data subjects or another person, or for the prevention or detection of a serious crime.

1.1.8 **Crime and Disorder Act 1998**

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police (through a DP2 application form process), Local Authorities, Probation Service or the Health Service but

only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

1.1.9 **The Computer Misuse Act 1990**

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual user's an individual user ID and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

1.2 **NHS Guidance**

1.2.1 **Confidentiality: NHS Code of Practice**

Provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their health information. It also details the required practice the NHS must take concerning security, identifying the main legal responsibilities for an organisation and also details employee's responsibilities

1.2.2 **Employee Code of Practice**

Guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff/employee and other individual's information

1.2.3 **Records Management: NHS and Health and Social Care Code of Practice**

Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc. Aids compliance with the Data Protection and Freedom of Information Acts

1.2.4 **ISO/IEC 17799 Information Security Standards**

This is the accepted industry standard for Information Management and Security. This standard has been adopted by all NHS organisations. It is also a recommended legal requirement under principle 7 of the Data Protection Act.

1.2.5 **No Secrets: 'Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse'.** This document gives guidance to local agencies who have a responsibility to investigate and take action when a vulnerable adult is believed to be suffering abuse. It offers a structure and content for the

development of local inter-agency policies, procedures and joint protocols which will draw on good practice nationally and locally.

1.2.6 **Mental Capacity Act 2005:** The act sets out how to assess a person to determine if they have capacity to make a specific decision at a specific time and how to determine their best interest if they lack capacity. It also sets out how to appoint a Lasting Power of Attorney, how the court of protection can appoint deputies to make specific decisions and the powers they have.

1.3 Purpose

1.3.1 This Policy aims to detail how Solent NHS Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are primarily based upon the key piece of legislation, the Data Protection Act 1998, however other relevant legislation and appropriate guidance will be referenced.

2 Scope & Definitions

2.1 Scope

This policy applies to bank, locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust and secondees (including students), volunteers (including Associate Hospital Managers), Non-Executive Directors, Governors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers and other workers who are assigned to Solent NHS Trust.

2.2 Glossary

DPA	Data Protection Act
IAC	Information Asset Custodian
IAO	Information Asset Owner
PID	Personally Identifiable Data
SIRO	Senior Information Risk Owner

2.3 Definitions

2.3.1 **Data:** Information which-

- is being processed by means of equipment operating automatically in response to instructions given for that purpose.
- is recorded with the intention that it should be processed by means of such equipment,
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system or,
- does not fall within above paragraph but forms part of an accessible record

2.3.2 **Data Controller:** The person or organisation (Solent NHS Trust) that collects personal data and decides on how to use, store or distribute that data.

2.3.3 **Data Processor:** Someone other than the Data Controller, who processes personal data on

their behalf.

2.3.4 **Data Subject:** An individual who is the subject of the personal data.

2.3.5 **Patient:** Throughout this document the term "patient" is used. This term includes those people who are also known as "Service Users", and "Clients".

2.3.6 **Personal Data:** Data that relates to and identifies a living individual that can identify the individual from this data or other information in the possession of the data controller.

2.3.7 **Sensitive Personal Data** Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

2.3.8 **Relevant Filing System:** A structured set of information that can reference individuals either directly or indirectly.

2.3.9 **Right of Subject Access:** 'Data Subjects' have the right to access and be given details of any information held about them that:

- 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.
- Please see Subject Access Guidance for more information

2.3.10 **Health Professional/Clinician:**

- a registered medical practitioner
- a registered dental care professionals as defined by section 53 (1) of the Dentists Act 1984,
- a registered optician as defined by section 36 (1) of the Opticians Act 1989,
- a registered pharmaceutical chemist and assistances as defined by section 24 (1) of the pharmacy Act 1954 or, a registered person as defined by Article 2 (2) of the pharmacy (Northern Ireland) Order 1976,
- a registered nurse, midwife or health visitor,
- a registered osteopath as defined by section 41 of the Osteopaths Act 1993,
- a registered chiropractor as defined by section 43 of the Chiropractors Act 1994,
- any person who is registered as a member of a profession to which Professions Supplementary to Medicine Act 1960 for the time being extends,
- a clinical psychologist, child psychotherapist or a speech therapist, a music therapist employed by a health service body and a scientist employed by such a body as head of a department.

3 Data Protection Act 1998

3.1 Data Protection Act 1998 - Principles and Practices to ensure compliance

The Trust will put in place procedures to ensure the Eight Principles in the Data Protection Act 1998 are met.

3.2 This Act applies to all person identifiable information held in manual files, computer databases, videos and other automated media, about living individuals. The Act dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.

3.3 The Act also requires Solent NHS Trust to register as a Data Controller with the Information Commissioners Officer; identifying the purposes for holding the data, how it is used and to whom it may be disclosed. Failure to register, an incorrect registration or an outdated registration, is a criminal offence. This may lead to prosecution of the organisation. The Trust's Data Protection Officer is responsible for maintaining the notification to the Information Commissioners Office.

3.4 All applications/databases required under law to be registered for data protection purposes will be registered under Solent NHS Trusts global registration with the Information Commissioner and does not need to be done individually

3.5 The Data Protection Principles, that Soelnt NHS Trust, all employers must adhered to are;

3.5.1 **Personal data shall be processed fairly and lawfully**

- Ensure that the proposed use of the information is lawful in the widest sense, e.g. doesn't breach other legal restrictions such as the common law duty of confidentiality.
- Inform patients why you are collecting their information, what you are going to do with it, and who you may share it with.
- Information recorded as part of the process of providing care should not be used for purposes that are unrelated to that care.
- There should be no surprises! Be open, honest and clear.
- The same principle applies to the personal information of staff.

Compliance with Data Protection and Caldicott will be achieved by implementing the following measures:

- Ensuring the organisation's Data Protection Notification is kept up to date.
- Complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.
- Ensuring that certain conditions in Schedules 2 and 3 of the Act are met. (*see Appendix A for detail of the Data Protection Act 1998 - First Principle*)

3.5.2 **To obtain personal data only for specified and lawful purposes and further process it only in a compatible manner.**

The following must be adhered to:

- Personal data must only be processed for the purposes for which it was originally obtained.
- Protocols should be in place to ensure that personal data that is passed on is used only for the purposes for which it was originally obtained.

- Only share information outside your organisation, team, ward, department, or service if you are certain it is appropriate and necessary to do so.

3.5.3 **Personal data must be adequate, relevant and not excessive**

- Only collect and keep the information you need.
- Do not collect information “just in case it might be useful one day!" You cannot hold information unless you know how it will be used and it is a justified use.
- Explain all abbreviations, use clear legible writing and stick to the facts – avoiding personal opinions and comments.

3.5.4 **Personal data must be accurate and kept up to date**.

- Take care when entering data to make sure it is correct.
- Data users recording information accurately and taking reasonable steps to check the accuracy of information they receive from data subjects or anyone else.
- Check existing records thoroughly before creating new records and avoid creating duplicate records.
- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information.

3.5.5 **Personal data must be kept no longer than necessary**.

This will be achieved by:

- Adherence to Records Management: NHS Code of Practice which is detailed in the Trusts Retention & Disposal of Records Policy.
- Staff working in joint team situations using the maximum retention period.

3.5.6 **Personal data must be processed in accordance with the rights of the individual**.

The Act gives seven rights to individuals, they are a:

1. **The right to subject access** – this allows people to find out what information is held about them on computer and within some manual records.
2. **The right to prevent processing** – anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else.
3. **The right to prevent processing for direct marketing** – anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.
4. **Rights in relation to automated decision-taking** – individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.
5. **The right to compensation** – an individual can claim compensation from a data controller for damage and distress caused by any breach of the Act. Compensation for distress alone can only be claimed in limited circumstances.
6. **The right to rectification, blocking, erasure and destruction** – individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion, based on inaccurate information.
7. **The right to ask the Information Commissioner to assess whether the Act has been contravened** – if someone believes their personal information has not been processed in accordance with the DPA, they can ask the Commissioner to make an assessment. If

the Act is found to be breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

Should an individual make a request to prevent processing then depending on the individual circumstances, the organisation would have to make a judgement based on the risk to the individual or others whether it was right to provide a service. Such requests should be directed to the Trust's Data Protection Officer

3.5.7 **Personal data must be kept secure**.

- This requires that all organisations that process personal information have security measures in place to ensure that the information is protected from accidental or deliberate loss, damage or destruction.
- Compliance will be achieved through the Information Security Policy and by following the Trust's guidance for sharing personal information. (See Appendix B)

3.5.8 **Personal data shall not be transferred to a country outside the European Economic Area unless that country can ensure adequate level of protection.**

- If sending personal information outside the European Economic Area (EEA), make sure consent is obtained where required and ensure the information is adequately protected.
- To ensure compliance protocols must be in place for the transfer of personal data outside the European Economic Area unless that country can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- Be careful about putting personal information on websites, which can be accessed from anywhere in the world - get consent first.
- Check where your information is going, and know where your suppliers are based.

3.6 Exemptions to the Data Protection Act 1998

In certain circumstances personal information may be disclosed and guidance is detailed below. However it is vital in each case, that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason.

3.6.1 Disclosing information against the subject's wishes

The responsibility of whether or not information should be withheld or disclosed without the subject's consent lies with the senior manager or senior clinician involved at the time and should be done in consultation with the Trust's Data Protection Officer and where applicable Caldicott Guardian and SIRO.

Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Child abuse and vulnerable adults
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of

drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

Reference: Confidentiality: NHS Code of Practice

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- Terminations - Abortion Regulations 1991, duty to inform
- Offenders thought to be mentally disordered – Mental Health Act 1983
- Child abuse – Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

3.6.2 The Confidentiality Code of Practice Supplementary Guidance for public interest disclosures including a decision matrix which can be found at Appendix D of this document.

Solent NHS Trust will support any member of staff who, using careful consideration, professional judgement and has sought guidance from the Trust's Data Protection Officer and can satisfactorily justify any decision to disclose or withhold information against a patient's wishes.

3.7 **Non–Disclosure of personal information contained in a Health record.**

An individual requesting access to their health records may be refused access to parts of the information if an appropriate Clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure should be documented. Where access would disclose information relating to or provided by a third party, consent for release must be given by the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed providing the identity of the third party is not revealed. The Act suggests that this might be done by omitting names and particulars from the records. Care should be taken to ensure that the information, if released is genuinely anonymous.

Further guidance is available from the Information Governance Team.

The organisation is not required to supply copies of health records if the individual requesting the information has

- not provided enough supporting information in order for the information to be located

- not supplied the appropriate fee
- not supplied the necessary evidence of identity

or

- the retrieval of the health records requires disproportionate effort

The **Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division), decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003** case identified guidance on issues of law concerning the right of access to personal data;

- what makes "data" "personal" within the meaning of "personal data"
- what is meant by a "relevant filing system"
- upon what basis should a data controller consider it "reasonable in all the circumstances" to comply with the request even though the personal data includes information about another and that other has not consented to disclosure

4 Caldicott Principles for handling person-identifiable data

4.1.1 Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

4.1.2 Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

4.1.3 Use the minimum necessary patient-identifiable information

Where the use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4.1.4 Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

4.1.5 Everyone with access to patient-identifiable information should be aware of their responsibilities

The organisation must ensure that those handling patient-identifiable information, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

4.1.6 **Understand and comply with the law**
Every use of patient-identifiable information must be lawful. The Caldicott Guardian is responsible for ensuring that the organisation complies with legal requirements.

4.1.7 **The duty to share information can be as important as the duty to protect patient confidentiality.**
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5 Confidentiality

The 'Confidentiality: NHS Code of Practice' has been published by the Department of Health following a major public consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

For the purposes of this document, the term 'staff ' is used as a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health. This includes private and voluntary sector staff.

This document

a) introduces the concept of confidentiality;
b) describes what a confidential service should look like;
c) provides a high level description of the main legal requirements;
d) recommends a generic decision support tool for sharing/disclosing information;
e) lists examples of particular information disclosure scenarios.

A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1-12), while the supporting Annexes provide detailed advice and guidance on the delivery of a confidential service.

The full document **Confidentiality: NHS Code of Practice** can be accessed from https://digital.nhs.uk/media/1157/Confidentiality-NHS-Code-of-Practice/pdf/Confidentiality-NHS-COP

5.1 Patient Confidentiality

5.1.1 Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a

degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

5.1.2 On admission or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.

5.1.3 In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

5.1.4 In the event a person lacks capacity to consent to information being shared staff should check if a person is authorised by a Lasting Power of Attorney (welfare) or been appointed by the court of protection to make that decision. The document must be seen. This person can consent on their behalf but must act in the person's best interest. If they have not then no one can consent on behalf of that person. A professional in the care team must assess if it is in the best interest of the person to share the information. The person's wishes and feeling, although not determinative, should be the starting point in this assessment. For further information see the Deprivation of Liberty and Mental Capacity Act policy.

In all cases, the wishes expressed must be appropriately documented in the patient's Health Records.

5.2 Staff Confidentiality

5.2.1 All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

5.2.2 Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager. Staff must not process any personal information in contravention of the Data Protection Act 1998.

5.2.3 Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

5.2.4 All staff have a confidentiality clause in their contract of employment. Solent NHS Trust has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

5.3 Breaches of Confidentiality

5.3.1 It is a breach of confidentiality to access, obtain or use personally identifiable data, without a justifiable reason to do so, as per Principle 1 of the Data Protection Act 1998.

5.3.2 It is a breach of the Data Protection Act 1998 for staff to unlawfully access, obtain or destroy their own personal data, without obtaining the data through lawful processes, as Solent NHS Trust is the Data Controller of this data.

5.4 Personal Identifiable Data in Medical Research

5.4.1 In order to ensure the key principles of Data Protection Act are adhered to, The Medical Research Council published guidelines on Personal Information in Medical Research (2000). It clearly states that the law assumes that whenever people give personal information to health professionals caring for them, it is confidential as long as it remains personally identifiable.

5.4.2 Frequently during medical research personal information is obtained from surveys, medical records, scientific tests and interviews. This information is confidential and any failure to control the ways in which it is used could be potentially harmful to a person's sense of security and self-confidence, the doctor-patient relationship or lead to unfair discrimination.

5.4.3 Since The Data Protection Act (DPA) 1998 (EU Data Protection Directive 95/46/EC) became law in 2000 researchers must also ensure their work is consistent with the law. However the law recognises that research which does not directly lead to decisions about a person should have special freedom to use information in ways not foreseen when it was collected but these uses must be fair and lawful.

5.4.4 All research within the Trust must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Development Department and undergo review through the Health Research Authority (HRA) process.

5.4.5 Research & Development Department will log and retain as appropriate, all relevant data protection agreements for research studies, as evidence for compliance with the DPA 1998 and Governance Toolkit.

6 Privacy Impact Assessment Procedure and Template

6.1.1 All projects and processes that involve personal information or intrusive technologies give rise to privacy issues and concerns. To enable the Trust to address the privacy concerns and risks a technique referred to a Privacy Impact Assessment (PIA) must be used. This process ensures that the Trust complies with the Data Protection Act: Principle 1 – *"Personal Data shall be processed fairly and lawfully"* and Principle 2 – "*Personal Data shall be processed for a specified purpose".* Refer to the Trust's Privacy Impact Assessment Procedure for details.

7 Roles & Responsibilities

Solent NHS Trust have established a structure to deliver information governance, to meet the requirements of data protection and confidentiality.

7.1 The Chief Executive

The Chief Executive has overall responsibility for Data Protection and Confidentiality within the Organisation. An accountable officer is responsible for the management of the

organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

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

The Chief Executive duties are to ensure:

- staff are aware of the need to comply with the Data Protection Act 1998, in particular with the rights of patients wishing to access personal information and or their health records.
- staff are aware of requirements of the common law duty of confidence as set out in Confidentiality: NHS Code of Practice.
- arrangements with third parties who process personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality.
- Local Research Ethics Committees and researchers are aware of the Data Protection Act and how it applies to the use of data for research purposes.

7.2 Senior Information Risk Owner (S.I.R.O)

The Senior Information Risk Owner (SIRO) has overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk.

7.3 Caldicott Guardian

The Caldicott Guardian is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of patient-identifiable information across the Trust and supporting agencies. To assist with the volume and diversity of this task the Caldicott Guardian is supported by the Information Governance Team, Information Asset Owners and Information Asset Custodians.

7.4 Data Protection Officer

The Data Protection Officer is part of the Information Governance Team. The Data Protection Officer has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance throughout the Trust with the Data Protection Act 1998.

The Data Protection Officer has these tasks:

- To promote awareness of the Act and Procedures contained in this policy
- To be responsible for compliance with the Act and the eight data protection principles.
- To ensure Trust compliance of Notification requirements with the Information Commissioner's Office
- To monitor changes to working practices, and where any such changes are found to come within the remit of the Act, to take appropriate action
- Liaise with the Information Commissioner's Office
- Be the first point of contact within the organisation for data protection and Caldicott issues

- Advise and update the Trust in relation to directives/guidance from the
- Information Commissioner and the Department of Health
- Via the Information Governance Framework – ensure that the Caldicott
- Guardian and Senior Information Risk Owner (SIRO) are informed of relevant issues and decisions are recorded
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation.
- Monitoring for actual or potential information security breaches.
- Ensuring that the Trust's personnel are aware of their responsibilities and accountability for information security
- Provide effective training for all staff in the requirements of Data Protection legislation and the Caldicott principles
- To liaise closely with the Information Asset Custodians and the Information Asset Owners.
- Carry out Data Protection and Caldicott compliance checks in departments, as required
- To help maintain the organisations Data Protection inventory by recording all service/local changes to the systems (both computerised and manual) inventory.
- Oversee applications for Subject Access and maintain appropriate files.

7.5 Information Security Specialist

The Information Security Specialist (provided by the Trust's ICT Provider) is responsible for:

- Monitoring and reporting on the state of ICT security within the organisation.
- Providing an advisory service on information security.

7.6 Information Asset Owners (IAO)

The Information Asset Owner (IAO) is a senior member of staff who is the owner for one or more identified information assets of the organisation.

There are several IAOs within the organisation, whose departmental roles may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

7.7 Information Asset Custodians

Information Asset Custodians, identified within each department of the organisation, are responsible for ensuring that the Data Protection and Caldicott principles are fully observed and complied with by staff within their department. They are required to ensure that all data flows and processing of data complies with all current Data Protection policies, working closely with Information Governance Team as appropriate.

Their tasks are to:

- Promote Data Protection & Caldicott Principles on an on-going basis, including posters, articles and local briefings
- Promote local induction and ensure that all new starters, before they access any information system, are given instruction on the Data Protection Act and Caldicott, as part of their first day/week induction programme.

- Ensure that all new staff attend the Corporate Induction session as soon as they are able
- Ensure all staff have access to current information on Data Protection Act and Caldicott requirements
- Ensure that all staff are aware of the Information Asset Custodian for their area and the contact details for the Information Governance Team
- Ensure that all staff know the procedure for reporting security incidents
- Ensure applications for access to systems within the department are processed following the agreed procedures and with appropriate authorisation
- Have systems in place to enable the above to be managed effectively within the service. Maintain close liaison with the Information Governance Team regarding any changes within the department

7.8 Compliance with Data Protection and Caldicott principles is a shared responsibility for all members of staff. By adhering to the principles, staff will help promote a secure environment where patients feel confident that their personal information is dealt with professionally and in accordance with the law.

8 Failure to Comply with the Policy

8.1 If a service feels it can not comply with all or part of an IG policy/ procedure they have a duty to undertake a risk assessment (Appendix E) which will be approved by the services Information Asset Owner and Information Governance Team. **Failure to do so could result in disciplinary action**. For further advice services should contact the Information Governance Team.

9 Training

9.1 All Trust staff will be made aware of their responsibilities for record-keeping and record management.

9.2 It is the responsibility of the Information Governance Team to provide Information Governance and Records Management training to all staff within the Trust.

9.3 It is mandated that all staff must complete assigned Information Governance and Records Management training annually.

9.4 Compliance with this training requirement will be monitored by the Learning & Development Team in conjunction with the Information Governance Team via a reporting mechanism learning and development training tool.

10 Equality & Diversity and Mental Capacity Act

A thorough and systematic assessment of this policy has been undertaken in accordance with the Trust's Policy on Equality and Human Rights.

The assessment found that the implementation of and compliance with this policy has no

impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation. See Appendix C

11 Monitoring the Effectiveness of the Policy

11.1 Information Governance Toolkit

The monitoring of this policy and its effectiveness and maintenance will be audited annually using the Information Governance Toolkit (IGT) or sooner if new legislation, codes of practice or national standards are introduced. The IGT audit is a self assessment audit undertaken by the Information Governance Team. In addition to this the IG Toolkit is audited annually by the Trust's Internal Auditors.

The owner/author of the policy is responsible for undertaking this audit and ensuring the policy's effectiveness. This will be monitored through the ICT Group to ensure effectiveness.

The implementation of this policy will be audited annually by the Information Governance Team who will also perform spot check audits to assess compliance.

Service Managers and Information Asset Custodians will work with the Information Governance Team to develop local action plans and monitor their completion. Service Managers and Information Asset Custodians will elevate risks identified through the Risk Register system.

The Information Governance Team will on a weekly basis review and monitor all Information Governance and Records Management incidents and were required conduct full investigations.

12 Review

12.1 This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

13 Reference and Links to Other Documents

This policy must be read in conjunction with the below policies that are available on the Intranet

Policies:

- Access to Records Procedure
- Data Encryption Policy
- Information Governance Policy
- Information Security Policy
- Records Management & Lifecycle Policy

Appendix A: Data Protection Act 1998 – The First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Schedule 2 conditions

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- The data subject has given their consent.
- For the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The process is necessary to protect the vital interests of the data subject.
- For the exercise of any other functions of a public nature exercised in the public interest.
- To pursue legitimate interests of the controller unless prejudicial to interests of the data subject.

Schedule 3 conditions for Processing Sensitive Data

- The data subject has given their explicit consent to the processing of the personal data.
- To comply with employers legal duty.
- In order to protect the vital interests of the data subject or another person, in a case where:-
    - Consent cannot be given by or on behalf of the data subject, or
    - The data controller cannot reasonably be expected to obtain the consent of the data subject, or
    - In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- The processing is carried out in the course of its legitimate activities by anybody or association which exists for political, philosophical, religious or trade-union purposes, and which is not established or conducted for profit, and is carried out with appropriate safeguards for the rights and freedoms of data subjects, and does not involve disclosure of the personal data to a third party without the consent of the data subject.
- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings).
- The processing is necessary for the purpose of obtaining legal advice, or
- The processing is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the

management of healthcare services) and is undertaken by:-
    - A health professional (as defined in the Act), or
    - A person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- The processing is of sensitive personal data consisting of information as to racial or ethnic origin, and the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality enabling such equality to be promoted or maintained, and the processing is carried out with the appropriate safeguards for the rights and freedoms of data subjects. The Secretary of State may by order, specify circumstances in which such processing is, or is not, to be taken to be carried out with the appropriate safeguards for the rights and freedoms of data subjects.

Interpretation

Personal data is not to be treated as being processed fairly unless the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made available to him at least:-

- The identify of the data controller;
- The purpose(s) for which data will be processed
- Any further information necessary.

Appendix B: Guidance for sharing personal information

Handling Confidential and Sensitive Information

The NHS constantly reviews how Personal Identifiable Data (PID) and Sensitive Data are transferred whether this is:

- in person
- post
- email
- telephone including text message
- removable devices including USBs, CDs, laptops, tablets, smartphones etc.
- fax
- other means

What is classified as PID and Sensitive Data?

This is to ensure transfers are secure and will protect the confidentiality of our service users and staff.

This guide sets out the steps you should take when sending, receiving or transporting information.

- Racial / ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences
- Bank, Financial Or Credit Card Details
- National Insurance Number
- Tax, Benefit Or Pension Records
- Health Records
- Adoption Records
- Employment Records
- Child Protection
- Name
- Address (home or business)
- Postcode
- NHS No
- Email address
- Date of birth
- Payroll number
- Driving Licence

Transferring Personally Identifiable Data (PID)

A step by Step guide on transferring PID can be found on the Intranet

Data Flow Mapping

An annual Data Flow Mapping Audit will be undertaken by the Information Asset Custodians to ensure compliance with this policy and awareness of all Personally Identifiable and sensitive Solent NHS Trust Data Flows

Appendix C: Equality Statement

Step 1 – Scoping; identify the policies aims	**Answer**
1. What are the main aims and objectives of the document?	To outline the process for Data Protection, Confidentiality and Caldicott Principles associated with standard operating procedures within Solent NHS Trust
2. Who will be affected by it?	All staff who are developing internal control documents
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	N/A
4. What information do you already have on the equality impact of this document?	None
5. Are there demographic changes or trends locally to be considered?	None
6. What other information do you need?	N/A

Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document unlawfully discriminate against any group?		x	
2. Can any group benefit or be excluded?		x	Applies to all staff groups
3. Can any group be denied fair & equal access to or treatment as a result of this document?		X	N/A
4. Can this actively promote good relations with and between different groups?		X	N/A
5. Have you carried out any consultation internally/externally with relevant individual groups?	X		Current Policy Steering Group members consulted and wider groups represented by PSG members..
6. Have you used a variety of different methods of consultation/involvement	X		Via email and face to face meetings
7. Mental Capacity Act implications			
8. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)	X		Does not apply to patients
9. What external factors have been considered in the development of this policy	X		Data Protection Laws
10. Are there any external implications to this policy	X		Non-compliance with Data Protection Laws – fines
11. Which external groups may be affected positively or adversely as a consequence of this policy being implemented	X		Patients - data

If there is no negative impact – end the Impact Assessment here.

Appendix D: Confidentiality NHS Code of Practice: Supplementary DoH Guidance Public Interest Disclosures – November 2010

Executive Summary:

This document expands upon the principles set out with the Department of Health's key guidance Confidentiality: NHS Code of Practice.

The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

Introduction

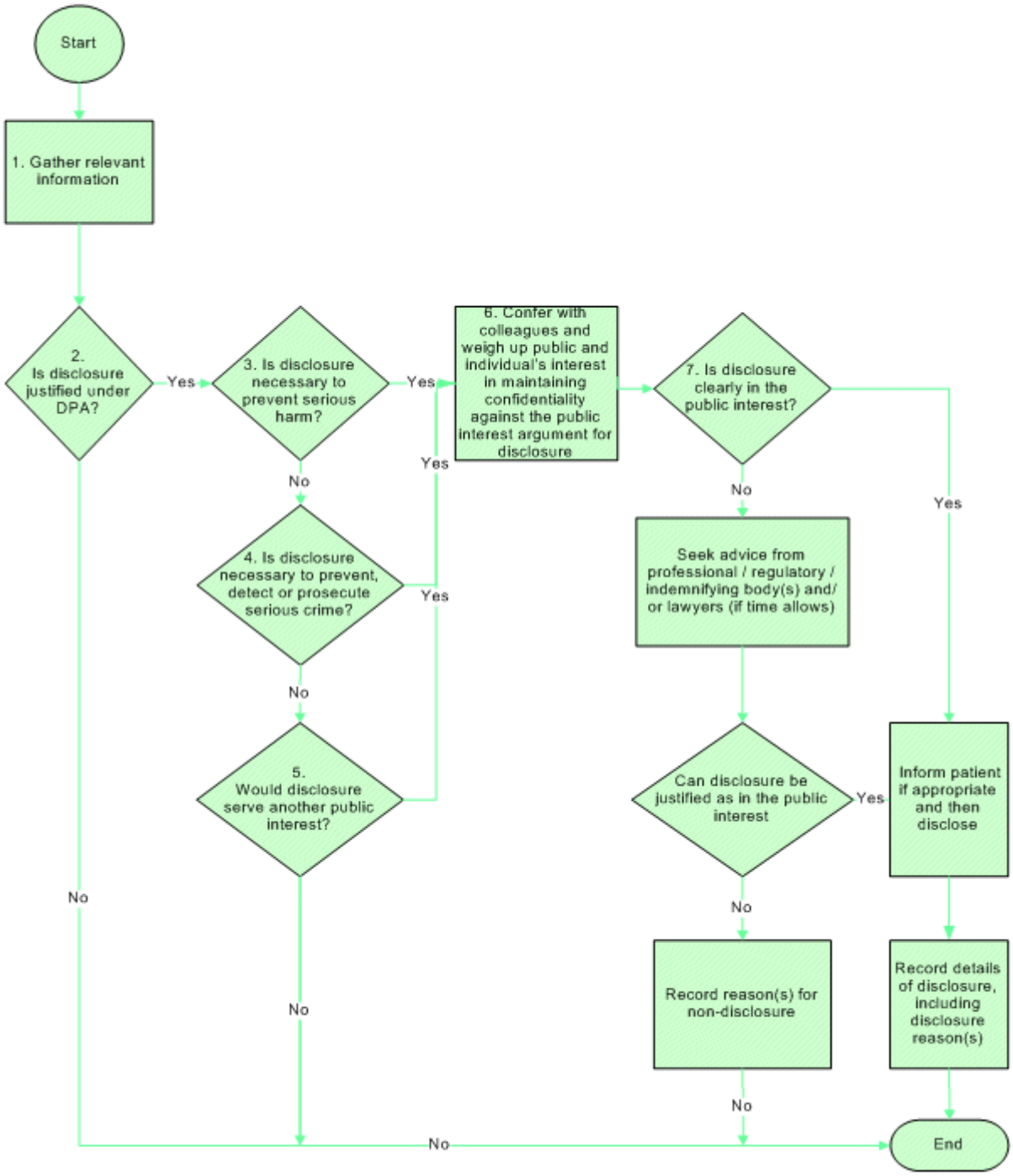
1. This document extends the guidance on disclosure of confidential information in the public interest that is contained within Annex B of the Department of Health's *Confidentiality: NHS Code of Practice*. Its purpose is to assist NHS staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest.

.

2. Decisions about disclosures of confidentially sensitive information must be made on a case-by-case basis. In considering whether to disclose information staff should consider the merits of each case however, certain considerations will need to be taken in all cases:
   - Extent of the information which is to be disclosed – *it will be easier to justify disclosure of demographic data or the fact that someone attended a clinic rather than detailed health information.*
   - The nature and impact of the crime or harm justifying the disclosure - *it will be easier to justify disclosure of information relating to a physical attack against a person than it would be for shoplifting.*
   - Whether the disclosure is for detection or prosecution of crime or harm to others or whether it is preventative - *it may be more justifiable to disclose information to support prosecution in relation to a crime that has occurred than to prevent a crime which has not yet occurred.*

3. A public interest justification for disclosure can be considered, and this guide becomes useful, in situations where:
   - Disclosure would be in the public interest; AND
   - The purpose of the disclosure cannot be achieved with anonymised information; AND
   - There is no statutory basis for disclosure; AND
   - Patient consent4 has not been given because:
     - It is not practicable to ask the patient(s) for consent e.g. because, for example, there are no up-to-date contact details for the patient, or the matter is urgent and the patient cannot be contacted; OR
     - It would be inappropriate to ask the patient(s) because, for example, they lack the capacity to give consent, or they are suspect(s) who should not be informed that they are under criminal investigation; OR
     - The patient(s) have been asked for consent and refused.

When might disclosure of confidential patient information without consent be justified in the public interest?



This flowchart contains decisions (diamonds) and actions (rectangles) describing the logic that can be followed when making public interest judgements. Where these decisions and actions merit further explanation, they are numbered and notes follow.

Notes on Flowchart

4. <u>Gather relevant information</u>
   It is important to begin by gathering relevant information to inform the public interest judgement to be made, such as:

- The purpose(s) served by the disclosure, and whether the purpose(s) could be served without the disclosure of confidential patient information;
- The individual(s) and/or organisation(s) affected by disclosure or non-disclosure, and the resulting level of detriment or benefit;
- The confidential information that is requested or required;
- The proposed recipient(s) of the disclosure, and whether they will disclose the information further;
- Whether there is either a statutory barrier or requirement to disclose;
- Who should be involved in the decision and who will be accountable; and
- The urgency of the decision.

5. The patient should be asked to consent to the disclosure (thus avoiding the need for public interest override) and/or for their perspective on the impact of disclosure (which can be helpful when weighing up whether to disclose), unless it is impractical to do so, or when contacting the patient would undermine the purpose of the disclosure.

6. Is disclosure justifiable under the DPA?
   Where confidential information is being disclosed for a purpose other than those identified as medical purposes in schedule 3 of the Data Protection Act 1998 then another justification must be found for the "processing". In practice, it will be very rare that such a justification will not be available as "functions of a public nature exercised in the public interest" is itself a schedule 3 justification, as are "administration of justice" and vital interests (matters of life and death).

7. Is the disclosure necessary to prevent serious harm?
   It is important to distinguish between serious harm to the individual to whom information relates and serious harm to others. Confidential information can be disclosed without consent to prevent serious harm or death to others. This is likely to be defensible in common law in the public interest.

8. Where the patient is an adult lacking capacity, the Mental Capacity Act applies, and the best interests of the patient concerned can be sufficient to justify disclosure, i.e. information can be disclosed to prevent a patient who lacks capacity from being harmed.

9. However, an individual's best interests are not sufficient to justify disclosure of confidential information where he/she has the capacity to decide for him/herself. There has to be an additional public interest justification, which may or may not be in the patient's best interests.

10. In some circumstance, e.g. where parents refuse to permit disclosure of information about a child who lacks capacity, clinicians should ultimately act in the best interest of the child.

11. Examples of where public interest can be a defence include:
    - Reporting to the Driver & Vehicle Licensing Centre a patient who rejects medical advice not to drive (although health professionals should inform the patient of their intention to report it);
    - Breaching the confidentiality of a patient who refuses to inform his or her sexual partner of a serious sexually transmissible infection;
    - Releasing relevant confidential information to social services where there is a risk of significant harm to a child.
12. Is disclosure necessary to prevent, detect or prosecute serious crime?

Confidential patient information can be disclosed in the public interest where that information can be used to prevent, detect, or prosecute, a serious crime. "Serious crime" is not clearly defined in law but will include crimes that cause serious physical or psychological harm to individuals. This will certainly include murder, manslaughter, rape, treason, kidnapping, and child abuse or neglect causing significant harm and will likely include other crimes which carry a five-year minimum prison sentence but may also include other acts that have a high impact on the victim.

13. On the other hand, theft, fraud or damage to property where loss or damage is not substantial are less likely to constitute a serious crime and as such may not warrant breach of confidential information, though proportionality is important here. It may, for example, be possible to disclose some information about an individual's involvement in crime without disclosing any clinical information.

14. In the grey area between these two extremes a judgement is required to assess whether the crime is sufficiently serious to warrant disclosure. The wider context is particularly important here. Sometimes crime may be considered as serious where there is a prolonged period of incidents even though none of them might be serious on its own (e.g. as sometimes occurs with child neglect). Serious fraud or theft involving significant NHS resources would be likely to harm individuals waiting for treatment. A comparatively minor prescription fraud might be serious if prescriptions for controlled drugs are being forged.

15. In some circumstances there may not be sufficient information available to determine whether or not a disclosure may serve to prevent or detect a serious crime. It may help to first hold an anonymised discussion with colleagues to establish whether concerns are justified and greater sharing of information is required may be appropriate.

16. Note that the public interest defence is separate from, and additional to, specific statutory requirements for disclosure in relation to crime. There is a legal duty to report financial assistance of terrorism, and legislation requires health professionals to release, where requested by police:
    - The names of patients treated after a car accident, to assist in the investigation of alleged dangerous driving;
    - Medical records / information, human tissue or fluid, if the request is backed by a court order or search warrant;
    - Medical records / information where there are reasonable grounds for believing the records are evidence in relation to an offence and it is necessary for police to seize them in order to prevent loss or alteration of evidence.

17. <u>Would disclosure serve another public interest?</u>
    There are clearly cases where disclosure of information may be in the public interest for a reason unrelated to serious harm or serious crime. The decision to disclose must take account of the likelihood of detriment (harm, distress or loss of privacy) to the individuals concerned, but a proportionate disclosure may be acceptable where there is clear benefit to the public. For example, a national clinical audit study into the effectiveness of a particular intervention may require the use of historic patient case notes where the majority of the affected patients are not contactable because they have since moved or died. There would be little or no detriment to the patients concerned and the public good resulting from the clinical audit may justify extracting

confidential information from the case notes. Similar considerations may apply to some research uses which do not affect the rights, freedoms or legitimate interests of individual patients.

18. However, since there is little case law in this area it is recommended that advice is sought from the National Information Governance Board (NIGB) before making such a disclosure. The NIGB advises the Secretary of State for Health on the use of powers provided under section 251 of the NHS Act 2006 that make it permissible to disclose, without consent, confidential data about groups of patients for "secondary" purposes where there is no clear public interest.

19. <u>Confer with colleagues and weigh up public and individual's interest in maintaining confidentiality against the public interest argument for disclosure</u>
The key factors in deciding whether or not to share confidential information are necessity and proportionality. The disclosure of confidential patient information must be necessary in order to satisfy an important public interest. Public interest must be judged on the merits of the case. Such a defence is only applicable in limited circumstances; public interest does not mean "of interest to the public".

20. There must be a balancing of the competing interests: the public interest achieved by the disclosure against both the potential damage caused to the individual whose confidentiality is to be breached and society's interest in the provision of a confidential health service. A fair balance should be struck between the rights of the patient, and the rights of other affected persons. Relevant factors to take into account are the potential damage to the care relationship between the health professional(s) and the patient, and the potential impact of the patient terminating that relationship. The health professional or another clinician must therefore be involved in the decision. Account should also be taken of the risk of a breakdown in trust between the patient and the NHS, and of the risk of loss of confidence amongst the public of the confidentiality of NHS services.

21. Health professionals must objectively assess public interest (e.g. through conferring with colleagues and by accessing independent advice) and not their own subjective views of what constitutes a public interest. Colleagues may identify additional factors to consider, and assist in weighing up the options. Where possible, the appropriate Caldicott Guardian should be involved. The identity of the patient should not be revealed in discussions. Seeking such advice may not be practicable in cases where the decision is urgent and there are no suitable colleagues available.

22. Health professionals may be protected by a public interest defence for disclosing information to avert a real risk of danger to the public, but they still have a duty of confidence and have to judge the most appropriate information and recipient of it to minimise detriment to the individual concerned. Disclosure should be to the appropriate person(s), and the confidential information provided should be limited to that necessary to fulfil the purpose of the disclosure. It may be possible to restrict the contents, recipient(s), or conditions of disclosure to limit the detriment caused but still achieve the public interest aim so that the disclosure is proportionate.

23. It will often be appropriate to place conditions on the recipient(s) of the disclosure e.g. that the confidential information is held securely and only used for a designated purpose and/or that it is not disclosed beyond specified limits.

24. Within the NHS Care Records Service, patients will be able to restrict access to their confidential information in various ways. In some circumstances, the opportunity will exist for clinicians to override the patient's restriction and access the restricted information, justifying their action in the public interest. This raises a different problem than in the normal case where a clinician discloses information to other person(s). The difficulty here is that the clinician will not know what information has been withheld and therefore what public benefit will be derived from access. This makes the weighing up of the benefits and disbenefits of disclosure difficult, but a public interest disclosure might still be justified.

25. Is disclosure clearly in the public interest?
In some cases, it will be clear that a proportionate disclosure is required in order to: Prevent serious harm being caused to one or more other individual(s), such as child abuse, or a serious assault;
    - Report a doctor or nurse with Hepatitis B who carries out exposure–prone procedures without taking proper precautions to protect patient safety; and/or
    - Prevent, detect or prosecute what is clearly a serious crime like murder or rape.

26. In other cases, further advice should be sought because it is less clear that a public interest defence is applicable. This might arise where, for example:
    - It is unclear whether the crime or harm is sufficiently serious to justify disclosure; or
    - A risk of serious crime or harm being committed exists but it is not clear whether the likelihood of it occurring is sufficient to justify the disclosure; or
    - A risk of serious crime or harm being committed exists but it is not clear whether it could be prevented without the disclosure (and thus whether the disclosure is "necessary"); or
    - Where harm is less severe but is prolonged (e.g. the impact on a child witnessing domestic violence over a long period);
    - Another important public interest other than preventing serious harm or serious crime would be served by the disclosure (e.g. a secondary use like research); or
    - The patient(s) have explicitly refused to consent to the disclosure, or
    - Some affected patients consent and some dissent to the disclosure; or
    - The benefit and detriment from disclosure are finely balanced.

Public Interest Exemplar Cases

Scenario 1: A receptionist at a GP surgery sees a patient leave the building and get into a car. On driving from the car park, the patient's car collides with and damages another patient's car. The driver does not stop, believing that nobody has seen the incident and instead drives away without leaving their details. Through her role at the surgery, the receptionist knows the identity of the patient.

Can the receptionist report the crime? What details can the receptionist provide about the accident and the driver?

Decision 1: A minor crime has been committed, but no serious crime or serious harm done. Therefore there is insufficient public interest (or any other) justification for revealing confidential patient information (e.g. from within the patient's case notes or even reveal that the patient had attended the surgery). However, a crime has been committed and the receptionist would be entitled

to report the incident, including the identity of the patient, to the police, but (s)he should not reveal confidential patient information.

Scenario 2: In one evening, at separate times, two patients enter an Accident & Emergency Department. Each of the patients has been a victim of a knife crime. Both patients report that they have been attacked by an individual and both describe what seems to be the same person. The patients claim that the attacks were unprovoked and that they did not know the attacker. The attacks happen within a mile of each other in a busy city centre. One of the patients is happy to speak to police and informs A & E staff of this. However, the other victim does not wish to have his information disclosed to the police because he does not want to be a police witness. He leaves before the police are called out.

Should the A & E staff report both incidents to the police? Should the identity of the patients and the details of the injuries be reported?

Decision 2: It is generally accepted that the reporting of knife and gun crimes will be within the public interest. A & E units should have standard procedures for informing the police that a knife crime has occurred. It should also be standard practice for staff to seek patient consent to involve the police. A knife attack may be sufficient to justify a public interest disclosure of confidential information even when consent is not given, where it is likely to assist in the prevention, detection or prosecution of a serious crime. Staff should ensure that they consider the proportionality of any disclosures. In this example, police could be called to interview the first patient, who could then be expected to identify himself, and provide a description of the attack and the attacker, and of his injuries. If the patient refused to provide some of these details, the hospital could provide them.

For the second patient, it is likely to be proportionate to provide the police with details of the patient, the attacker, the attack and the patient's injuries.

Scenario 3: One day during surgery hours a GP notices Mr Smith arrive, park his car and enter the surgery building. Mr Smith had attended an appointment in the previous month with the GP. At a previous appointment, the GP had prescribed Mr Smith with drugs and informed him that they were likely to make him drowsy, and that he should avoid driving. During the consultation Mr Smith had assured the GP that he'd "be fine!" when accepting the prescription. The GP knows Mr Smith well, and that he might ignore advice not to drive, and so has some concern over whether Mr Smith was fit to drive.

What action should the GP take?

Decision 3: In principle, Mr Smith could cause serious harm to others by continuing to drive. The GP should speak to Mr Smith and try to establish whether his medication is having the effect of making him drowsy and unfit to drive, and if so, to encourage him once more to stop driving. Discussion with colleagues may assist the GP in assessing the risk posed to the public from the effect of Mr Smith's medication, and in weighing up whether a breach of confidence is justified. If Mr Smith is unfit to drive but nevertheless persists in driving, it would be justifiable in the public interest to inform the Driver and Vehicle Licensing Agency.

Scenario 4: Mrs Jones arrives at the Accident & Emergency Department with a number of cuts and bruises and stab wounds of some kind (from a screwdriver or penknife). She is very shaken up and anxious. Whilst treating the patient, A & E staff discover that this is the third time in three months that Mrs Jones has presented at A & E with injuries. It is also noted that Mrs Jones has a ten year-old son. She tells the staff that she is very clumsy and keeps having accidents. However, the injuries this time are not consistent with a clumsy accident, and the A & E staff are concerned that she may be the victim of assault, and that her son might also be at risk.

What should A & E staff do?

Decision 4: With further discussion and reassurance, Mrs Jones may reveal the true cause of her injuries. It may help if A&E staff explain that they believe her injuries are not consistent with her story. If Mrs Jones does admit that she is being assaulted by someone she lives with or sees regularly, then it will be easier for staff to decide whether they need to take any action to protect the child, such as notifying social services. This action could be justifiable in the public interest if it was considered that there was a risk of serious harm to the child. If Mrs Jones was prepared to admit to the cause of the violence and take action to safeguard the child, then it may not be considered necessary to inform social services. Such cases are often difficult and advice and guidance from a Caldicott Guardian and child protection advisor is likely to be helpful.

Scenario 5: A patient has been arrested on suspicion of robbery and the police have asked a consultant psychiatrist for a 'background' report based on prior knowledge. The police do not explain any more about the nature of the alleged crime but say they will use the report when preparing the papers for the Crown Prosecution Service. The consultant has not been asked to assess the patient and is not convinced that the patient would consent to the disclosure of information.

Should the consultant provide the report?

Decision 5: The consultant's decision hinges on whether robbery is a serious crime. Were the police to not provide further details (e.g. as to whether it is robbery with violence), it would be reasonable for the consultant to assume this does not constitute a serious crime. Without a court order, the police can not force the consultant to provide a report. However, in this case, the police disclose that the robbery was with serious violence, and the consultant judges this to be an investigation of a serious crime. The consultant consults the Caldicott Guardian and another colleague. They consider whether the public interest in disclosure outweighs the potential damage from the disclosure. In this case, they feel that the patient's relationship with the psychiatrist (and with any future psychiatric services the patient may receive) would be seriously damaged by a disclosure. Furthermore, the patient receives services through an outreach centre, and the doctors fear that this may lead to other patients withdrawing from the outreach services. They judge that no report should be provided without the patient's consent.

Scenario 6: Following a series of complaints to a Member of Parliament from local residents, all of whom suffer from a particular disease and live close to a nuclear power station, a project is set up to investigate whether the proximity to the power station could contribute to the onset of the disease. The investigation team from the Public Health Observatory seeks access to confidential information within approximately two thousand paper case notes in Newtown Hospital Trust in order to discover the prevalence of relevant symptoms. The team argues that it is not feasible to seek consent from patients within the timescales of the enquiry and that their work can be justified in the public interest.

Decision 6: The Newtown Hospital Trust Caldicott Guardian considers that the risk of serious harm is not sufficient to breach the confidence of thousands of patients. However, she feels there is a strong public interest in the investigation. In order to minimise the potential detriment caused, she offers to assist the investigation by providing local clinical coding staff to extract relevant data from the case notes and provide it to the investigation team. Nevertheless, the data to be provided could still reveal patient identity, and so she instructs the investigation team that the information provided must be stored and processed securely, and that no identifiable patient information will be published without explicit patient consent.

Appendix E: Information Governance Risk Assessment

GENERIC RISK ASSESSMENTS – Information Governance

		Likelihood of a risk occurring as a result of non-compliance with policy				
		1	2	3	4	5
		Rare	Unlikely	Possible	Likely	Almost Certain
Severity is a risk was to occur	5 Catastrophic	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

- This assessment must be undertaken for any current activity that does not meet policies and/or procedural standards and therefore deemed to present a significant risk to employees, patients, visitors or the organisation.
- **The assessment should be reviewed and signed by the departmental Information Asset Owner and approved by the Information Governance Team** **InformationGovernanceTeam@solent.nhs.uk**
- **Assessing a risk: Likelihood (L) x Severity (S) = Risk (R)**
  - Very Low (Green) = Risk is to be managed locally by the departmental Information Asset Custodian ;
  - Low (Yellow) = Risk is to be managed locally by the departmental Information Asset Custodian, although the Information Governance Team should be contacted for advice on actions to be taken in order to mitigate the risk;
  - Moderate (Orange) = Risk is to be managed jointly with the responsible Information Asset Owner and Information Governance Team, a detailed risk reduction plan must be completed;
  - **High (Red) = Current practice should be suspended until a detailed assessment has been undertaken and a Risk Reduction Plan developed and implemented, as it could present a significant risk to the organisation. Risk is to be managed jointly with the Information Asset Owner and Information Governance Team.**

- When considering the Risk Reduction Plan, the following should be considered (not limited to); avoid current practice if possible, assess those activities that cannot be avoided, reduce the level of risk to the lowest level reasonably practicable by looking at alternative practices, training, etc.

Information Governance Activity e.g. unable to comply with policy, transferring of data, relocation of data, service relocation, etc…	**Group Affected** e.g. breach of confidentially for an employee, patient, client, etc…	**Reason for non-compliance/ risk** e.g. unable to ensure security of data, transferring data in incorrect method, relocation of data due to service relocation, no identified process, etc…	**Existing Control Measures** What has the service already put in place to reduce the risk of non-compliance/risk	**Degree of Risk**			**Additional Mandated Actions Required to Reduce the Level of Risk** To be completed by the Information Asset Owner and Information Governance Team	**Residual Risk**		
				L	**S**	**R**		**L**	**S**	**R**

Signed …….. **Signed** ……..

Print Name …….. **Print Name** ……..

(Information Asset Owner) **(Information Governance Team)**