NHS
Solent
NHS Trust

Information Governance Policy

Purpose of Agreement	Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. This policy serves to underpin those areas of Information Governance that The Trust is working toward.
Document Type	[x] Policy [ ] SOP [ ] Guideline
Reference Number	IG01
Version	4
Name of Approving Committees/Groups	ICT Group Policy Steering Group
Operational Date	March 2018
Document Review Date	March 2021
Document Sponsor (Name & Job Title)	Chief Operating Officer & SIRO
Document Manager (Name & Job Title)	Data Protection Officer and Head of Information Governance and Security
Document developed in consultation with	ICT Group Policy Steering Group
Intranet Location	Polices & Procedures Page, Information Governance Page
Website Location	FOI Publication Scheme 'Our Policies & Procedures'.
Keywords (for website/intranet uploading)	Information Governance Policy, IG Policy, Governance, Information Governance Toolkit

Amendments Summary:

Amend No	Issued	Page	Subject	Action Date
1		Appendix B	Inclusion of IG Risk Assessment	November 2010
2			Change of name to Solent NHS Trust , Change to Sponsor Name.	October 2011
2		12	Update CRG	October 2011
2			General Review – minimal changes	March 2013
2	December 2016		General Review – minimal changes	November 2016
3	January 2018	Minor amendments	Minor amendments	January 2018

Summary

This policy outlines both the Trust's and Staff's obligation to ensuring that data held by the Trust remains restricted and secure and is only used for its intended purpose.

It covers;

- IG Principles – In accordance with the Data Protection Act 1998
- IG Framework – this is based upon compliance with the IG Toolkit Requirements
- Legal and Regulatory Compliance – The Trust identifies awareness and compliance with all Information Laws
- Information Security – covers the restriction and security of all information held by the Trust, that is either personally identifiable or deemed sensitive.
- Incident Investigation – Ensuring all IG Breaches are investigated appropriately and that where incidents are graded as a Level 1 (High Risk Incident) or Level 2 (Serious Incident Requiring Investigation), a higher level of investigation is undertaken
- Information Quality & Records Management – Ensuring the standards required for records held, are adhered to and monitored.
- IG Training – Ensuring all staff are effectively trained on an annual basis

Table of Contents

1 Introduction & Purpose

1.1 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It is integral to clinical governance, service planning and performance management. Information Governance ensures necessary safeguards for, and appropriate use of, patient and personal information.

1.2 Key areas are information policy for health and social care, IG standards for National Programme for IT systems and development of guidance for NHS and partner organisations.

1.3 The purpose of this policy is to set out a system that ensures The Trust meets its responsibilities in the management of information assets and resources.

2 Aim of the Policy

2.1 The Trust will at board level establish and support an Information Governance Management Framework (as defined in requirement 8-101) of accountability. This framework will deliver:

- The responsibility for IG and this policy
- The associated strategy and Improvement plan

3 Scope

3.1 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.

3.2

3.3 **Information Governance is** based on six standards that represent aspects of information handling. The six standards (below) of the Information Governance Toolkit split the requirements into manageable divisions, highlighting interfaces, where appropriate. The standards are:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

3.4 The standards are applicable to:

- All information used by The Trust (Patient/Client/Service user information/Staff, etc…)
- All information managed by The Trust
- Any individual using information 'owned' by The Trust
- Any individual requiring access to information 'owned' by The Trust

3.5 This policy covers all aspects of information within The Trust including but not limited to:

- Structured records systems – paper, electronic
- Transmission of information – email, fax, telephone or post.

3.6 This policy covers all information systems purchased, developed or managed by/or on behalf of the organisation.

4 Principles

4.1 The Trust's Information Governance principles are:

- To hold information securely and confidentially
- To obtain information fairly and efficiently
- To record information accurately, reliably and in a timely manner
- To use information in decision making effectively and ethically
- To share information appropriately and lawfully with other health organisations and agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.
- To recognise the balance between openness and confidentiality

4.2 The Trust fully supports corporate, clinical and information governance and recognises its duty of public accountability whilst equally upholding security and confidentiality to safeguard personal information relating to patients and staff and commercially sensitive information. Where it is in the interest of the patient or the public interest, the organisation recognises the need to securely share information with other health and social care organisations, including agencies, in a controlled manner where it is deemed to be in the best interest of the individual. This does not change the rights of patients to the protection of their confidentiality in accordance with Article 8 of the Human Rights Act, the Data Protection Act and at 'common law'.

5 The Information Governance Management Framework

5.1 Information will be defined and where appropriate kept confidential, underpinning the principles of 'Caldicott' and the Data Protection Act 1998.

5.2 Freedom of Information and Openness

5.3 Non-confidential information within The Trust and its services should be available to the public through a variety of media, including the Trust Publication Scheme in line with the Freedom of Information Act 2000, which replaces the open government code of practice and the NHS code of practice, in place since 1994.

5.4 The Trust has established and maintains policies and procedures to ensure compliance with the Freedom of Information Act 2000.

5.5 The Trust will regularly undertake reviews of its policies and arrangements for openness.

5.6 Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients (access to records policy). Except where it may be impracticable, unlawful or undesirable to do so.

5.7 The Trust has clear procedures and arrangements for liaison with the press and broadcasting media via the Communications team.

5.8 The Trust has clear procedures and arrangements for handling queries from patients and the public.

6 Legal and Regulatory Compliance Framework

6.1 There are a number of legal obligations placed upon The Trust regarding the use and security of all identifiable personal information.

6.2 There are also requirements for appropriately disclosing information when required please see the Data Protection Act, Schedule 29.3 Disclosure to Police in the 'prevention and detection of serious crime'.

6.3 The Trust will undertake reviews of its compliance with legal requirements and relevant codes of conduct in line with operating procedures and codes of practice adopted within the NHS.

6.4 The Trust regards all identifiable personal information relating to patients and staff as confidential except where national policy on accountability and openness requires otherwise (e.g. Freedom of Information Act 2000)

6.5 The Trust will establish and maintain a protocol and relevant information sharing agreements for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

6.6 The Trust will establish and maintain policies to ensure compliance with:

- The Public Records Act 1958 & 1967
- Copyright Designs & Patents Act 1988
- Data Protection Act 1998
- Human Rights Act
- The Computer Misuse Act 1990
- Freedom of Information 2000 & Environmental Information Regulations 2004
- Mental Capacity Act 2005
- the Common law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Records Management NHS Code of Practice
- Caldicott Guidance
- Current Performance Standards - NHS IG Toolkit
- No Secrets Act 2000
- Children's Act 1989
- The Protection of Children Act 1999
- Safeguarding Adults & Safeguarding Children

7 Information Security

7.1 The Trust has established and maintained policies for the effective and secure management of its information assets and resources.

7.2 The Trust will undertake or commission annual reviews and audits of its information and IT security arrangements

7.3 The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training. Including but not limited to the use of NHS mail for all Personally Identifiable Data (Patient/Staff) and sensitive data for external email communications.

7.4 The Trust will undertake risk assessments to determine that appropriate security controls are in place for existing or potential information systems.

7.5 The Trust will use BS7799 as the basis of its Information Security management arrangements.

7.6 Incident management within The Trust is established through Information Governance incident reporting procedures; to enable the monitoring and investigation of all reported instances of actual or potential breaches of confidentiality and security.(Requirements 301, 302, 307 and in compliance with the Information Governance risk management policy).

7.7 All information security incidents must be advised to the Information Governance Team and sent/recorded with the Risk Management Team, in line with the Information Security Policy, who will then pass onto the Information Governance Team for specialist investigation.

7.8 Breach of this policy will lead to disciplinary action, including dismissal.

8 Reporting, Managing & Investigating Serious Incidents Requiring Investigation (SIRI's)

8.1 Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. Reference should be made to the Forensic Readiness Policy and where applicable contact made with the Local Fraud Team

8.2 The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

8.3 These incidents must be reported using the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf

9 Information Quality Assurance & Records Management

9.1 The Trust has established and maintains policies and procedures for information quality assurance and the effective management of records.

9.2 The Trust will undertake or commission regular annual assessments and audits of its information quality and records management arrangements.

9.3 Managers and Information Asset Owners in keeping with the specification of their job description are accountable for the continual improvement of the quality of information within their services and to ensure effective records management through the Information Asset Custodians

9.4 Wherever possible, information quality and records management should be assured at the point of collection.

9.5 Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

9.6 The Trust will promote information quality and effective records management through policies, procedures/user manuals, Induction training and mandated annual Information Governance Training

9.7 Data Input staff should ensure verification of the information entered is audited on a regular basis.

10 Roles & Responsibility: Reporting Structure for Key Governance Bodies

10.1 It is the role of the Trust Board to approve the organisations policy and implement the Information Governance Management Framework, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy and the supporting Information Governance Management Framework Strategy.

10.2 Quality Improvement & Risk Group is responsible for monitoring compliance with;

- IG Compliance
- IG Audits
- IG Policy Compliance

10.3 ICT Group is responsible for monitoring compliance with;

- IG Toolkit Compliance
- ICT Security Compliance
- Cyber Security
- ICT / IG Issues and Breaches

10.4 SIRI Panel is responsible for monitoring compliance with;

- IG Security Breaches

10.5 The above groups will also be responsible for developing and maintaining the Information Governance improvement action plan, policies, standards, procedures and guidance (in accordance with relevant service areas), coordinating Information

Governance in the organisation and raising awareness of Information Governance. These groups will monitor this policy and will report regularly through the Senior Information Risk Owner (SIRO) to Trust Board.

10.6 The Trust Information Governance Management Framework its roles and accountabilities are defined within the Information Governance Strategy.

11 Policy Approval

11.1 The Trust's policy group acknowledges that information is a valuable asset, therefore it is in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

11.2 This policy, and its supporting standards and work instruction, are fully endorsed by the Board through the production of these documents and their minuted approval.

11.3 All staff, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of the Trust objectives and the delivery of effective healthcare to the local population.

11.4 This policy will be available on the intranet or alternatively distributed by the IG Team. Information Asset Owners and Information Asset Custodians shall also be issued with a copy. The communications team shall also advise all staff of this policy and its location.

12 Failure to Comply with the Policy

12.1 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 B) 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.

13 Training Requirement (IG 112)

13.1 It is the responsibility of the Information Governance Team to provide/monitor Information Governance, Information Security, Freedom of Information and Records Management training to all new starters (Inclusive of Junior doctor's intake) Agency, bank & volunteers within the Trust as part of the IG Training programme.

13.2 The Trust ensures that appropriate training is made available to staff and completed as necessary to support their duties

13.3 Full details of our training resources are available within our supporting IG Strategy document.

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

14 Equality & Diversity and Human Rights

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

14.2 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)

15 Success Criteria/Monitoring the effectiveness of the Policy

15.1 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 IG Toolkit audit is a self-assessment audit undertaken by the Information Governance Team; additionally the submission is audited annually by internal auditors.

15.2 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 and bespoke team training where deemed to be required.

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

15.4 The implementation of this policy will be audited annually by the Information Governance Team via Information Asset Custodians and all staff. The Information Governance Team will also perform spot check audits to assess compliance in compliance with IG toolkit requirements.

16 Review

16.1 This document may be reviewed at any time at the request of either staff side or management, but will be reviewed three years unless organisational changes, legislation, guidance or non-compliance prompt an earlier review

17 References and Links to Other Documents

17.1 This policy must be read in conjunction with the below policies that are available on the Intranet http://solent/corp/igov/Lists/IG%20Policies/AllItems.aspx

Policies:

- Access to Records Procedure
- Audio Visual Records Policy
- Data Encryption Policy
- Data Protection, Caldicott and Confidentiality Policies & Procedures
- Information Governance Policy
- Information Security Policy
- FOI Policy
- Records Management & Lifecycle Policy

Other Documents:

- Information Governance http://www.connectingforhealth.nhs.uk/systemsandservices/infogov
- Human Rights Act http://www.crimereduction.homeoffice.gov.uk/hra.htm
- Trust Policies & Procedures
- The Information Commissioner www.ico.gov.uk
- FOI Act www.ico.gov.uk

Appendix A: Operating Framework Care Record Guarantee 2011/12 Revision V5

Definitional Notes

Original Metric Definition:
Each provider organisation should have an organisational IG policy framework that delivers the obligations set out in the Care Record Guarantee (CRG)

N.B. There is an illustrated leaflet about care records for young children, which can be downloaded from the above site.
The 12 CRG Requirements are:

1. When we receive a request from you in writing, we must normally give you access to everything we have recorded about you. We may not give you confidential information about other people, or information that a healthcare professional considers likely to cause serious harm to the physical or mental health of you or someone else. This applies to paper and electronic records. However, if you ask us to, we will let other people see health records about you.

   Wherever possible, we will make your health records available to you free of charge or at a minimum charge, as allowed by law. We will provide other ways for you to apply to see your records if you cannot do so in writing.

   We will provide information in a format that is accessible to you (for example, in large type if you are partially sighted).

2. When we provide healthcare, we will share your record with the people providing care or checking the quality of care (unless you have asked that we limit how we share your record). Everyone looking at your record, whether on paper or computer, must keep the information confidential.

   We will aim to share only as much information as people need to know to play their part in your healthcare.

3. We will not share health information that identifies you (particularly with other government agencies) for any reason other than providing your care, unless:
   - you ask us to do so;
   - we ask and you give us specific permission;
   - we have to do this by law;
   - we have special permission for health or research purposes; or
   - we have special permission because the public good is thought to be of greater importance than your confidentiality.

   If we share information without your permission, we will make sure that we keep to the Data Protection Act 1998, the NHS confidentiality code of practice and other national guidelines on best practice.

4. Legally, no-one else can make decisions on your behalf about sharing health information that identifies you. The only exceptions to this are parents or legal guardians, or people with legal powers to make decisions on behalf of adults who cannot make the decision for themselves or who may be a risk to others. You can appoint someone to have a lasting power of attorney to make decisions for you if you are losing the ability to make decisions for yourself. You can decide what rights that person has in making decisions about your care record. If you do not appoint anyone, a senior healthcare professional involved in your care may consider it to be in your best interests to share information. This judgment should take account of the views of your relatives and carers, and any views you have already recorded. For medical research or other purposes (see the box on page 6), the National Information Governance Board for

Health and Social Care advises when special permission should be given to share any health information that could identify individuals.

5. Sometimes your healthcare will be provided by members of a care team, which might include people from other organisations such as social services or education. We will tell you if this is the case. When it could be best for your care for your health information to be shared with organisations outside the NHS, we will agree this with you beforehand. If you don't agree, we will discuss with you the possible effect this may have on your care and alternatives available to you.

6. Usually you can choose to limit how we share the information in your care records which identifies you. In helping you decide, we will discuss with you how this may affect our ability to provide you with care or treatment, and any alternatives available to you.

7. We will deal fairly and efficiently with your questions, concerns and complaints about how we use information about you. All trusts have a Patient Advice and Liaison Service (PALS) which can answer questions, point people towards sources of advice and support, and advise on how to make a complaint. We will have a clear complaints procedure. We will use what we learn from your concerns and complaints to improve services.

8. We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We will normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you feel you are suffering distress or harm as a result of information currently held in your record, you can apply to have the information amended or deleted.

9. 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.

   All organisations providing care for the NHS or on our behalf must follow the same strict policies and controls. This is managed through the Department of Health's Information Governance Framework for Health and Social Care, and through the individual standards which make up the Information Governance Toolkit.

10. 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.

    There may be times when someone will need to look at information about you without you giving your permission first. This may be justified, for example, if you need emergency care.

11. We will keep a record in the newer electronic record systems of anyone who has accessed a health record or added notes to it. Some of the older computer systems will only record who has accessed a record where they have made changes. Paper records only include where people have made notes in the record and not when someone looks at the record.

12. If you believe your information is being viewed inappropriately we will investigate and report our findings to you. If we find that someone has deliberately accessed records about you without permission or good reason, we will tell you and take action. This can include disciplinary action, which could include ending a contract, firing an employee or bringing criminal charges.

Appendix B: 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)**

Appendix C: Impact assessment

Step 1 – Scoping; identify the policies aims	**Answer**
1. What are the main aims and objectives of the policy?	To set out this organisations policy in respect to Information Governance.
2. Who will be affected by it?	All staff and other users.
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	IG Toolkit requirements assessment. To maintain and improve our Information Governance Toolkit Scores and to raise awareness of Information Governance to all so that they may act in compliance with the requirements in the execution of their duties.
4. What information do you already have on the equality impact of this policy?	None
5. Are there demographic changes or trends locally to be considered?	N/A
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 policy unlawfully be used discriminate against any group?		x	Policy
2. Can any group benefit or be excluded?		x	N/A
3. Can any group be denied fair & equal access to or treatment as a result of this policy?		X	
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		ICT Group Policy Steering Group
6. Have you used a variety of different methods of consultation/involvement	X		Face to face meetings and via email/post
7. Mental Capacity Act implications			
8. Will this policy require a decision to be made by or about a service user? (Refer to the Mental Capacity Act policy for further information)		x	N/A
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