Data Protection Risk Management Operational Procedure

Solent NHS Trust O-SOPs can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	To provide staff with clear guidance of the management of Data Protection Risk, in accordance with the Trust's Data Protection Compliance Policy, Data Protection Legislation and Trust Risk Management Policies and Processes
Document Type	Organisational Wide Standard Operating Procedure (O-SOP)
Linked to Policy	IG23 Data Protection Compliance Policy
Reference Number	Solent NHST / O-SOP / IG23.3
Version	V1
Name of Approving Committees / Groups	Policy Steering Group, Clinical Executive Group
Operational Date	May 2022
Document Review Date	May 2025
Document Sponsor (Job Title)	Rachel Cheal, Senior Information Risk Owner
Document Manager (Job Title)	Sadie Bell, Data Protection Officer
Document developed in consultation with	Head of Quality & Safety
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	N/A
Keywords (for website / intranet uploading)	Risk Management, Data Breach, Incident, O-SOP, IG23.3

Review and amendment log

Version Number	Review date	Amendment section no.	Page	Amendment made / summary	Changes approved by

Table of Contents

Data Protection Risk Management Operational Procedure

1. INTRODUCTION & PURPOSE

This procedure sets out the approach taken within Solent NHS Trust for the management of Information Governance Risk.

Whilst the Trust's Risk Management Framework and associated risk management policies are applicable to all risks, this procedure identifies those additional measures which are specific to the management of information risks. This refers to all information held in electronic, paper-based or any other format, whether stored in automated or manual systems. This will encourage proactive risk management, aid, and improve the quality of, decision making throughout the Trust and help to safeguard the Trust's information assets.

The procedure ensures that all managers and staff are aware of and comply with the Trust's statutory obligations and responsibilities regarding information risk, including those under the Data Protection Act (DPA), and the General Data Protection Regulations (UK GDPR).

Solent NHS Trust has ensured through this procedure that appropriately senior individuals are allocated responsibility for owning information risk within the organisation this is embedded through a hierarchical Information Governance Framework structure. (See fig 1)

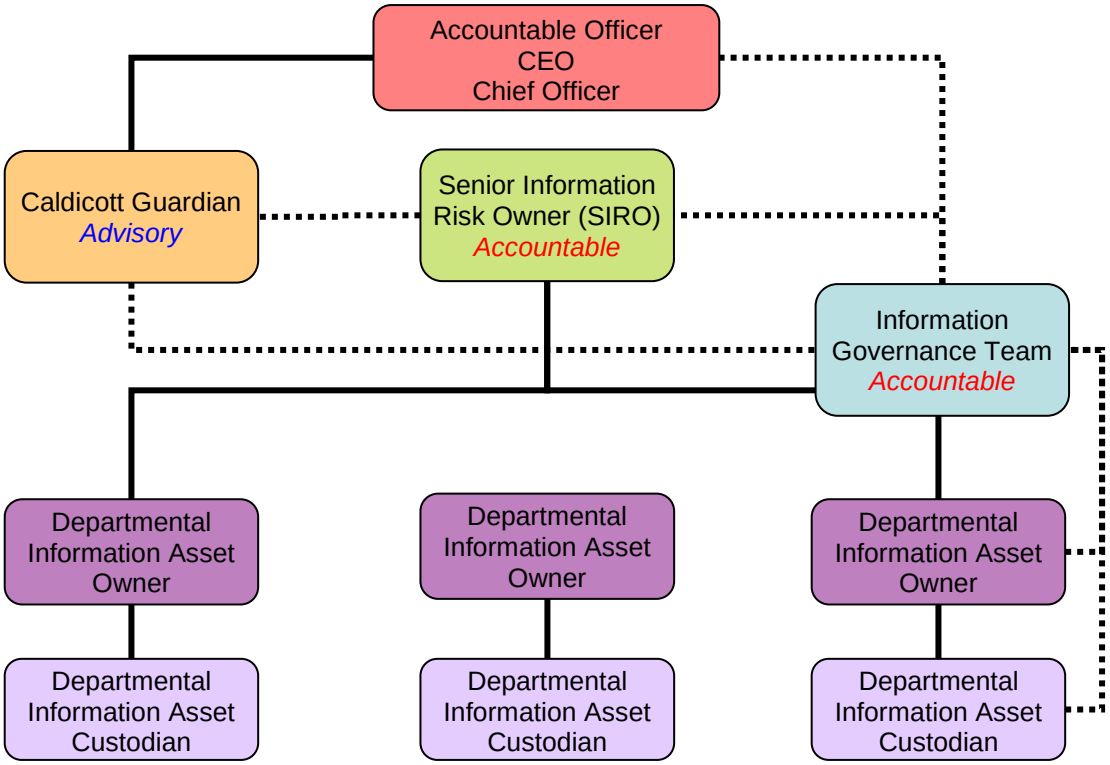

fig 1

This structure within Solent NHS Trust is underpinned and upheld by the Senior Information Risk Owner (SIRO). The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the board (or equivalent senior management group/committee).

Information Governance risk is inherent in organisational activities. Information Governance risk management is the ongoing process of identifying information risks and implementing plans to address them.

The Solent NHS Trust Board have approved the introduction and embedding of Information Governance risk management into the key controls and approval processes of all major business processes and functions of the organisation. This decision reflects the high level of importance placed upon minimising Information Governance risk and safeguarding the interests of patients, clients and staff Information Governance risk within the organisation.

The Solent NHS Trust Board recognises that the aim of Information Governance risk management is to strive to eliminate and / or reduce risk, by provision of a structural means to identify, prioritise and manage the risks involved in all activities. This requires a balance between the cost of managing and treating Information Governance risks with the anticipated benefits that will be derived.

The Solent NHS Trust Board acknowledges that Information Governance risk management is an essential element of broader Information Governance and is an integral part of good management practice. The intent is to embed Information Governance risk management in a very practical way into business processes and functions. The intention is for this to be achieved through approval and review processes / controls, and not to impose Information Governance risk management as an additional requirement.

This procedure is applicable throughout all services and departments and functions in Solent NHS Trust, that collect, transmit, or retain information in any form and adherence should further be included in all contracts for outsourced or shared services, in respect to Data Controllers, Data Controllers in Common, Data Processors and Data subjects. There are no exclusions.

Risk management

2. PROCESS

2.1. Information Risk Framework

Solent NHS Trust Chief Executive (the Accountable Officer) has delegated responsibility for the oversight and implementation of Information Governance risk management to a senior advisor of the organisations Board.

Solent NHS Trust Senior Information Risk Owner (SIRO) is responsible for and familiar with Information Governance risks and the approach taken within Solent NHS Trust, to ensure the organisation can provide the necessary mitigation and support to the Board and in so doing to the Accountable Officer.

This Board member nominated as SIRO has undertaken strategic Information Governance risk management training.

The SIRO will own the development and maintenance of Information Governance risk management policies, procedures and standards, act as an advocate for information risk on the board and in internal discussions and provide written advice to the Chief Executive on the content of the Statement of Internal Control relating to information risk. The SIRO is responsible for the ongoing development and day-to-day management of the organisation's Information Governance Risk Management Programme for information privacy and security.

The SIRO will with assistance from the Information Governance Team and nominate Information Asset Owners (IAOs) at an appropriate senior level to be ascribed to Information Assets.

IAOs will take appropriate actions to:

- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Ensure that information risk assessments are performed quarterly on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency
- Ensure that Information Governance security accreditation is maintained by undertaking at least yearly reviews of the system level security policy for critical systems owned
- IAOs shall submit the risk assessment results and associated mitigation plans to the Information Governance Team for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks
- IAOs shall complete an overarching annual report to the SIRO
- IAOs shall be responsible for developing a Business Continuity Plan for their assets which shall be reviewed on an annual basis

The Information Governance hierarchical risk supporting infrastructure within the organisation, is to provide support for the SIRO and will consist of the organisation's Caldicott Guardian, the Data Protection Officer and Head of Information Governance and Security and Information Communication Technology Group. The Information Communication Technology Group will on behalf of the Solent NHS Trust Board be the committee responsible for the oversight and assurance of the processes for the identification and assessment of Information Governance risk.

Everyone in Solent NHS Trust has a role to play in the effective management of Information Governance risk. All staff will participate in the mandated annual Information Governance training in compliance with the training needs assessment matrix, Information Governance Team and actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate mitigating actions under advisement of the Information Governance Team.

2.2. Reporting of Data Protection Incidents

Staff provide the Trust's first line of defence against information loss and theft, and therefore all staff must be able to spot common activities where information could be lost and know what to report. A breach does not necessarily need to involve the loss or disclosure of personal information in order to be treated as a data security incident. These are the different categories that breaches, and incidents can fall into:

- Cyber Security
- Inappropriate Access / Disclosure
- Lost / Missing PID
- Lost Smartcard / ID
- Non-Encrypted Email Used for PID
- PID Found in Public Place
- Other IG Incident (only use if this incident is rare)
- PID in wrong Record / Record Error
- PID Saved / Stored Insecurely
- PID Sent to Wrong Person / Address

All data breaches and near-misses must be formally reported as soon as possible via the Trust's incident reporting system. Where the breach involves the inappropriate destruction or alteration, loss / theft, or unauthorised disclosure of (or access to) data, the Information Governance Team must be informed immediately (ideally via telephone) to assess the severity of the breach and support with identifying the remedial action required.

Data protection legislation draws a distinction between a "data controller" and a "data processor" in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. All contracts with third parties should have clear clauses and expectations regarding the reporting of data breaches. In the case of any data breach, the identified data controller must be notified as soon as possible.

The Trust is required to document all data breaches and near misses, including details of the breach itself, its' effects, and the remedial action taken. This information is centrally recorded within the Trust's adverse incident reporting system.

2.3. Data Protection Investigation Process

All Data Protection incidents will be reviewed and scored in accordance with NHS Digital's; "Guide to the Notification of Data Security and Protection Incidents"
https: / / www.DSPToolkit.nhs.uk / Help / Attachment / 148

Depending on the outcome of the review, an incident will either be identified as a local incident, a High-Risk Incident, or a Serious Incident. The Data Protection incident level will determine the type of incident investigation that should take place and who should be involved and / or notified.

If an incident is identified as a High Risk or Serious Incident an investigation will be undertaken, in accordance with the Trust's Incident Reporting, Investigation and Learning Policy.

As a result of the investigation a formal report will be written, and an action plan identified. The Information Governance Team will monitor all open action plans relating to Data Protection incidents on a monthly basis, following up with action leads until the action has been completed.

2.4. Notification of Data Protection Breaches

Local Investigation incident report

The following will be involved in the incident investigation;

- Reporter
- IG Team
- Governance Lead / Professional Standards Lead
- Information Asset Custodian (if required)

The following will be informed of the incidents after the investigation;

- Information Asset Owner (Monthly incident reports)
- Senior Information Risk Owner (Annual Report)

High Risk Incident (HRI) Investigation

The following will be involved in the incident investigation;

- Reporter
- IG Team
- Governance Lead / Professional Standards Lead
- Information Asset Custodian (if required)
- Information Asset Owner

The following will be informed of the incident and advise may be sought from;

- Caldicott Guardian
- SIRO

Serious Incidents (SI)
The following will be involved in the incident investigation;

- Reporter
- IG Team
- Governance Lead / Professional Standards Lead
- Information Asset Custodian (if required)
- Information Asset Owner
- Associate Director
- Caldicott Guardian
- SIRO

The following will be informed of the incident and advise may be sought from;

- CEO

The incident will be reported, using the DSPT Online Toolkit and consequently the following will be notified of the incident and a formal report will need to be shared with;

- The Information Commissioners Office
- NHS Digital
- Commissioners

It is important to deal with breaches quickly, effectively, and appropriately. A strategy for dealing with the breach should be formulated as soon as possible, in conjunction with the Information Governance Team and any other appropriate Teams (such as IT, HR etc), which should include:

a) a recovery plan (including damage limitation);
b) assessing the risks associated with the incident;
c) informing the appropriate people / organisations that the incident has occurred; and
d) reviewing and updating information security to avoid further incidents.

All breaches and near-misses should be fully investigated, and staff should be able to identify any lessons which can be learnt and any measures which can be put in place to avoid the breach happening again. This might involve a change in process or equipment or introducing additional data security or check mechanisms. Other possible remediation options can be discussed with the Information Governance Team

High Risk Incident
All Data Protection incidents within Solent NHS Trust meeting the High-Risk category in accordance with NHS Digital's guidance for scoring Data Protection incidents, are to be measured against a checklist to determine if a formal or informal investigation will be carried out.

It may be agreed and determined at the incident review meeting, that no additional learning will be identified as a result of a formal investigation, due to a number of factors, e.g. the incident was the result of an unintentional human error, the incident was a result of failure to follow process, this was an isolated event specific to a service and all actions were taken immediately, etc. Under these circumstances, no formal investigation report will be required to be undertaken by services. The Information Governance Team will monitor these incidents within a consolidated report to Serious Incident panel, to highlight incidents, ensuring awareness of data breaches and allow preventative work to be undertaken within the Trust.

Serious Incident – Notification: As soon as Solent NHS Trust becomes aware that a personal data breach has occurred, the Information Governance Team will notify the personal data breach to the ICO without undue delay and, where feasible, not later than 72 hours of the Trust having become aware of it, unless able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of Data subjects. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Solent NHS Trust are required to report Data Protection incidents via the DSPT (notifying the ICO) within 72 hours once notified of an incident (within this time, a view meeting must take place to determine if the category meets a level 2 or above)

Solent NHS Trust should communicate a personal data breach to the data subject, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the Data subject in order to allow him or her to take the necessary precautions. Solent NHS Trust's Duty of Candour procedures should be followed when notifying individuals of personal data breaches.

Notifying Data Subjects: The Trust must always consider its' duty to inform the affected data subjects without undue delay, unless the Trust can demonstrate that:

- It has "implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption"; or
- It has "taken subsequent measures which ensure that the high risk to the rights and freedom of data subjects is no longer likely to materialise"; or
- Any communication to the data subjects on an individual basis "would involve disproportionate effort". If this situation occurs, the Trust is expected to issue general public communications "whereby the data subjects are informed in an equally effective manner".

As part of the Trust's Duty to Inform requirements, and its' commitment to promote a culture of being open and transparent, it is encouraged that data subjects should be notified of all data breaches involving their information, regardless of whether it was externally reportable.

Where it is expected / agreed that data subjects are to be contacted, this communication must describe the nature of the breach in clear and plain language, and should include the information specified

Human Resources – Improving & Managing Conduct Policy: If an IG breach should lead to a member of staff being investigated through the Improving & Managing Conduct Policy, the Data Protection Officer / Head of Information Governance and Security (or appointed delegate) should be consulted with as a professional advisor as necessary during the investigation process. The Data Protection Office / Head of Information Governance and Security will consult with the Senior Information Risk Owner (SIRO) and / or Caldicott Guardian, as accountable officers for IG Breaches. The SIRO and Caldicott Guardian must always be notified of the outcome summary of the disciplinary e.g. no action, verbal warning, official warning, retraining, etc., so that the Information Commissioners Office can be advised, as this is a requirement of their investigation process.

Counter Fraud - Suspected fraud, bribery and/or corruption linked to data breaches should be reported to the Trusts Local Counter Fraud Specialist and will be investigated in line with

the Trust Local Fraud, Bribery and Corruption Policy and NHS Counter Fraud Manual. The SIRO and Caldicott Guardian must always be notified of the outcome of the fraud investigation e.g. no action or criminal prosecution so that the Information Commissioners Office can be advised.

Transparency about Information Risk: Solent NHS Trust promotes transparency about its' Information Governance risks, incidents and lessons learned and publishes information setting out how it handles information and a summary material on Information Risk issues in the Trusts Annual Governance Statement, within its' Annual Report.

2.5. Learning from Data Protection Breaches

A key outcome of any investigation would be to establish learning and change practice. In addition to undertaking this when a High Risk or Serious Incident occurs, the Information Governance Team will undertake the following processes, to establish learning:

- Every month the Information Governance Team will identify the most commonly reported type of incident. Once identified the team will contact services who have reported this type of incident and conduct a piece of service engagement. The aim of the service engagement is to look into the incidents in more detail, gain the perspective of the service as to what their business needs are surrounding the incident, what happened leading up to and as a result of the incident and what process changes can be introduced. As a result of the service engagement, a process change options document will be produced and cascaded to all services. It is important to have several process options identified, recognising and reflecting on the diverse service needs across the organisation.

- Annually, a deep dive incident review will be undertaken by the Information Governance Team and reported to the Board, in accordance with requirement 4.1.1 of the Data Protection & Security Toolkit; this will be reported as part of the Board's Information Governance Report to Board. The aim of this is to assess the Trust's Data Protection incidents as a whole, reflecting on the type of incidents reported in the last 12 months, the actions taken and what strategic action may need to be taken to prevent future reoccurrences. This is a top-level review, underpinned by the monthly local incident reviews and the reviews undertaken on a daily basis, when assessing incidents.

2.6. Data Protection Risk Management Processes and Prevention of Breaches

Solent NHS Trust will be vigilant in the protection of all personal data whose release or loss could cause harm or distress to individuals.

Solent NHS Trust will identify, risk assess and manage appropriately data they or any

third-party contractor holds whose release or loss could cause harm or distress to individuals. It will handle all such information as if it were at least "PROTECTED – PERSONAL DATA" while it is held, processed, or stored within this organisation or that of its' partners, applying the measures outlined within this policy and strategy. This will include as a minimum, all data falling into one or both categories below.

A. Any information that links one or more identifiable living person with information about them, which if released would put them at significant risk of harm or distress.

B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.

Information Governance Risk assessments are undertaken for all Solent NHS Trust Clinical and Corporate critical information systems and critical information assets. Information Governance Risk / Data Protection Impact Assessments will occur at the following times:

- At the inception of new systems, applications, facilities, changes to process etc. that may impact the assurance of Solent NHS Trust Information or Information Systems Data Protection Impact Assessments (DPIAs) will be completed. These DPIAs will be brought with supporting documentation to the Information Communication Technology Group for consideration and review.
- Ideally DPIAs should be completed before enhancements, upgrades, and conversions associated with critical systems or applications (Information Security Policy)
- When NHS policy or legislation requires risk determination
- When the Solent NHS Trust organisation Management team / Board requires it

The Solent NHS Trust organisation will undertake an annual information Data Flow Mapping exercise and from this exercise, determine the information risks regarding its' data flows within the organisation and or with its' delivery partners. An annual report on Data Flow Mapping including recommendations and mitigating actions will be reviewed by the Information Communication Technology Group and approved by the SIRO

Information Governance incident reporting will follow the same processes embedded within the organisation's overall risk management approach and suite of Policies.

Solent NHS Trust will undertake and publish Data Protection Impact Assessments as part of its' Information Governance risk management programme for all new projects, systems, and research proposals.

2.7. Third Party Contractual Obligations

Solent NHS Trust will ensure that all contracts with Third Parties, include the standard NHS generic IG model contracts clauses with regards to the Data Protection Act and Information Governance Breaches. In compliance with Freedom of Information requirements, contracts will not contain privacy clauses.

3. EQUALITY IMPACT ASSESSMENT

A thorough and systematic assessment of this procedure 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 procedure has no impact on any Trust employee on the grounds of age, disability, gender, race, faith, or sexual orientation.

4. REVIEW

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.

5. REFERENCES AND LINKS TO OTHER DOCUMENTS

- NHS Digitals Guide to the Notification of Data Security and Protection Incidents https: / / www.dsptoolkit.nhs.uk / Help / Attachment / 148
- Data Protection Compliance Policy
- Privacy by Design Procedure
- Incident Reporting, Investigation and Learning Policy

6. GLOSSARY

Abbreviation	Full Name
CEO	Chief Executive Officer
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit
FOI	Freedom of Information
GDPR	(UK) General Data Protection Regulations
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
O-SOP	Organisational Wide Standard Operating Procedure
PID	Personally, Identifiable Data
SIRO	Senior Information Risk Owner