Livewell Southwest

Information Governance Strategy

Version No 2.1

Notice to staff using a paper copy of this guidance.

The policies and procedures page of LSW Intranet holds the most recent version of this document and staff must ensure that they are using the most recent guidance.

Author:	**Information Governance Lead & Information Governance Group**
Asset Number:	**815**

Reader Information

Title	Information Governance Strategy. V.2.1
Asset number	815
Rights of access	Public
Type of paper	Strategy
Category	Non Clinical
Document purpose/summary	This strategy sets out Livewell Southwest's CIC Information Governance framework to help ensure compliance with all appropriate legislation, standards and best practice for both current and future management of information
Author	Information Governance Lead & Information Governance Group
Ratification date and group	24th February 2016. Policy Ratification Group
Publication date	3rd March 2016
Review date and frequency (one, two or three years based on risk assessment)	To be reviewed annually in line with any significant changes to mandatory requirements, national guidance or as a result of significant information governance breaches or incidents
Disposal date	The Policy Ratification Group will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation
Job title	Information Governance Lead
Target audience	All LSW staff
Circulation	Electronic: Livewell Southwest (LSW) intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☏ 01752 435104. Please contact the author if you require this document in an alternative format.
Consultation process	Information Governance Group
Equality analysis checklist completed	Yes
References/sources of information	• Access to Health Records (1990) • Compute Misuse Act (1990) • Data Protection Act (1998) • Human Rights Act (1998) • Freedom of Information Act (2000)

	• Confidentiality: NHS Code of Practice (2003) • The Common Law Obligation of Confidentiality • DH: Information Governance Toolkit V.13 (Health & Social Care Information Centre) - https://www.igt.hscic.gov.uk • DH: NHS IG - Information Risk Management - Good Practice Guide (2009) • DH: Caldicott Guardian Manual (2010) • Health and Social Care Act (2012) • DH: Information: To Share or Not to Share? The Information Governance Review (2013)
Associated documentation	• Audiovisual Recordings of Patients/Visitors/Staff and Business Activities Policy • Clinical Record & Note Keeping Policy • Communications Systems: Phone, Email, Internet & Fax Policy • Data Protection, Confidentiality, Caldicott & Safe Haven Policy • Disclosure of Health Records • Freedom of Information & Environmental Information Regulations Guidance • Incident Reporting and Investigation Policy • Information Governance Policy • IT Security Policy • Privacy Impact Assessment Policy • Records Management Policy • Risk Management Policy • Security Policy • Template for developing Data Sharing Agreements
Supersedes document	Information Governance Strategy V1.0
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon. PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version No.	Type of change	Date	Originator of change	Description of change
1	New strategy	March 2012	Information Governance Manager	New strategy
2	Reviewed	April 2014	Information Governance Manager	Reviewed
2.1	Reviewed	December 2015	Internal audit	Reviewed and Inclusion of reference to SystmOne at Appendix A

Contents		Page
1	Purpose of this strategy	5
2	Information Governance principles	5
3	Aims and objectives	5
4	Scope of the strategy	6
5	Legal and Regulatory Framework	7
6	Management structure and responsibilities	7
7	Key Components of the strategy	9
8	Delivering Information Governance	10
9	Monitoring and Review	10
Appendix 1	Process flowchart for the ratification of policies	12

Information Governance Strategy

1 Purpose of this strategy

1.1 Information Governance (IG) is framework for ensuring that the necessary safeguards for, and appropriate use of personal confidential information.

1.2 This strategy sets out LSW Community Interest Company's (LSW) approach for providing a robust IG framework to comply with all relevant legislation, standards, best practice.

2 Information Governance principles

2.1 LSW recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Importance is placed on the confidentiality of, and the security arrangements to safeguard, both personal confidential information about patients, staff and commercially sensitive information.

2.2 The organisation also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

2.3 LSW believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

3 Aims and objectives

3.1 Information Governance is a vital component for 'keeping people safe, well and at home' and underpins LSW's strategic five aims:

- To be a recognised employee led organisation.
- Based around local people and communities.
- Providing seamless system leadership.
- Where experience exceeds expectations.
- Sustainable, successful and admired.

The aims of this document are to ensure that data are:

- **H**eld securely and confidentially.
- **O**btained fairly and efficiently.
- **R**ecorded accurately and reliably.
- **U**sed effectively and ethically.
- **S**hared and disclosed appropriately and lawfully.

Based on the Department of Health's model for managing information (HORUS Model).

3.2 This strategy sets out seven main objectives:

- To achieve a high standard of excellence for information governance.
- To ensure individuals take personal responsibility for all aspects of information governance.
- To ensure policies, procedures, guidelines, monitoring, audits and training enable high quality information governance.
- To minimise and manage key information governance risks.
- To ensure information governance complies with statutory and regulatory requirements and compliance frameworks including the Department of Health (DH) Information Governance Toolkit and the Care Quality Commission.
- To routinely improve information governance standards whilst responding to the changing needs of LSW, legislation, compliance frameworks and any other initiatives where information governance is a key element.
- To embed information governance seamlessly into the governance of LSW.

4 Scope of the strategy

4.1 The DH Information Governance Toolkit reflects the IG framework through six main components which include:

- Information governance management.
- Confidentiality and data protection assurance.
- Information security assurance.
- Clinical information assurance.
- Assurance for secondary uses of information.
- Corporate information assurance.

See Appendix One.

5 Legal and Regulatory Framework

5.1 LSW will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and common law confidentiality.

5.2 LSW will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

6 Management structure and responsibilities

6.1 LSW Board

- It is the role of LSW Board to define the organisation's policy in respect of IG and meeting legal, statutory and NHS requirements.
- LSW has appointed a Senior Information Risk Owner (SIRO) at Board level who has clearly defined Board level responsibility for overseeing all the diverse aspects of IG, information risk and information security within LSW. The SIRO is the Director of Professional Practice, Safety and Quality.

6.2 Senior Information Risk Owner (SIRO)

- The SIRO is responsible for and takes ownership of the organisation's IG/risk policy and acts as advocate for IG risk on the Board.
- Authorises the IG Toolkit self-assessment submissions and ensures that an effective information assurance governance infrastructure is in place.
- This includes information asset ownership, reporting, defined roles and responsibilities.

6.3 Caldicott Guardian

- The Caldicott Guardian acts in a strategic and advisory capacity in the use and sharing of patient information.
- Responsible for approving, monitoring and reviewing protocols governing access to person identifiable information by staff within LSW and other organisations both NHS and non NHS.
- This role is undertaken by the Medical Director.

6.4 Information Governance Group

- Responsible for ensuring there is a robust IG management framework to support the current and evolving IG agenda within LSW.
- This includes monitoring compliance of the IG Toolkit, developing and maintaining policies, standard procedures and guidance, raising awareness of IG across the organisation.
- Reports by exception to LSW Safety, Quality & Performance Committee on IG issues and IG risk.
- Membership of the group:

    - Senior Information Risk Owner, IG Lead & Chair (Director of Professional Practice, Quality & Safety)
    - Caldicott Guardian (Medical Director)
    - Records Management, Data Protection & Deputy Chair (IG & Records Manager)
    - Operations Management (South West Locality Manager)
    - Information Technology & Security (PHNT ICT Security Manager)
    - Workforce Development (Information Asset Owner)
    - IT Systems (Information Asset Owner)
    - Business Continuity (Risk Management representative)
    - Internal Audit

6.5 Information Governance Lead

- Responsible for leading the work of the Information Governance Group, co-ordinating the various strands into a comprehensive work programme to ensure LSW meets its statutory and regulatory obligations.
- Supports the SIRO and Caldicott Guardian in the IG agenda, provides advice and guidance to LSW on matters relating to IG and responsible for the timely completion and submission of the end of financial year DH IG Toolkit self-assessment.

6.6 Information Asset Owner (IAO)

- An information asset is a body of information that has value to the organisation, its business operations and its continuity.
- Information Asset Owners are senior individuals who are responsible for identifying, understanding and addressing risk to the information assets they ‘own’.
- Accountable to the SIRO for providing assurance on the security and use of their information assets.

6.7 Information Asset Administrator (IAA)

- Information Asset Administrators are System Managers who are familiar with the information asset within their area and are responsible for ensuring that that policies and procedures are followed and recognise actual or potential security incidents of the asset.

6.8 Information and Communication Technology (ICT) Security Coordinator

- Responsible for coordinating information technology security for LSW.

6.8 Managers

- Responsible for ensuring that IG policies, procedures, standards and guidelines are built into local processes and that there is on-going compliance.

6.9 All staff

- All staff, whether permanent, temporary or contracted, including students, contractors and volunteers shall comply with LSW IG policies and procedures to ensure that no breach of information security or confidentiality result from their actions.

6.10 Third party contractors/third parties

- Appropriate contracts and confidentiality information security agreements shall be in place with third party contractors/third parties where potential or actual access to information assets is identified.

7. Key Components of the strategy

- An annual action plan arising from a base line assessment against the standards set out in the DH IG Toolkit which will be a key vehicle for improving IG within LSW.

- A management framework and robust infrastructure which will support the implementation, monitoring and review of IG within LSW.

8. Delivering Information Governance

8.1 LSW will develop and maintain a robust management and responsibility reporting structure to ensure that IG and associated risks are appropriately managed to support the overall risk management function within LSW.

- Formation of a dedicated Information Governance Group.
- Appointment of the key roles and responsibilities.
- Informing staff and key personnel and their responsibility?
- Provision of clear advice and guidance throughout the organisation.
- Implementation of defined information incident reporting and investigating procedures linked to the risk management process.

8.2 All staff must understand and apply best practice and the principles of IG to manage all information to support the business activities of the organisation. This will be achieved through:

- Delivery of mandatory IG training both at induction and an annual update for all staff.
- Regular communications to staff using LSW staff bulletins, intranet and management team briefs.
- Signing of confidentiality clauses within all staff contracts.
- Publication of IG policies, procedures and guidance on LSW intranet.

8.3 LSW will ensure that clear advice and guidance explaining how information is recorded and shared and how any concerns may be raised. Information will also be provided on Subject Access Requests (SAR) under the Data Protection Act 1998.

8.4 LSW will undertake regular reviews and audits of how information is used through:

- Mapping of data flows.
- Review of reported information incidents.
- Data quality checks.
- Ad hoc IG spot checks on compliance with best practice.

9. Monitoring and Review

9.1 The Information Governance Group will monitor implementation of this strategy and its associated work programmes through regular meetings. LSW is mandated to complete a self-assessment of its IG performance using the IG Toolkit. This is an on line assessment based on 39 IG standards and LSW's work programme will be developed against the IG Toolkit which will identify risks, issues of improvement and good practice.

9.2 The Information Governance Group will formally review this strategy every three years however the content will be reviewed annually to include any significant changes to mandatory requirements, national guidance or as a result of significant information governance breaches or incidents in order to ensure that all types of information are more effectively managed within LSW.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice, Safety & Quality

Date: 1st March 2016

Appendix One: Overall Information Governance Framework (Based on the IG Toolkit)

	100 Series – IG Management	200 Series – Confidentiality/Data Protection Assurance	300 Series – Information Security Assurance	400 Series – Clinical Information Assurance	500 Series – Secondary Use Assurance	600 Series Corporate Information Assurance
Policies	• IG Policy • IT Security Policy • DP, Confidentiality, Caldicott • & Safe Haven Policy • Disclosure of Health Records Policy • Clinical Record & Note Keeping Policy • Appraisal Policy	• IG Policy • DP, Confidentiality, Caldicott & Safe Haven Policy • Disclosure of Health Records Policy • Privacy Impact Assessment Policy • Audiovisual Recordings of Patients/Visitors/Staff & Business Activities Policy	• Phone, Email, Internet & Fax Policy • IG Policy • IT Security Policy • Risk Mgt. Policy • Business Continuity & Recovery Policy	• Records Mgt. Policy • ePEX Policy & Coding Manual • SystmOne Policy • Clinical Audit Policy	• ePEX Policy & Coding Manual • SystmOne Policy	• FOI Guidance • Records Mgt. Policy
Related documents	• IG Strategy • IG Implementation & Action Plan • IG Training Programme • IG contract clauses • IG Quarterly Reports • Job Descriptions • Terms of Reference • Minutes of Meetings	• Log of Caldicott Issues • Privacy Impact Assessment Notice • IG Leaflets/Posters • Subject Access Request Process • Data Sharing Agreements	• Registration Authority Handbook • List of Info. Assets • Log of Remote Access Requests • System Level Security Policies • Statements from PICTS	• Terms of Reference • NHS Number Action Plan • ePEX Training Manual • SystmOne Policy • Records Mgt. Reports • Minutes of Meetings • SystmOne Guidance	• ePEX Training Manual • SystmOne Policy	• Log of FOI Requests • Corporate Records Inventory
Committees/ Working Groups	• IG Group • Audit Committee	• IG Group		• ePEX Governance Group • SystmOne Strategy Group • CPA & MH Records Group • Children & YP Health Record Group • Records Administration Group • Community & Rehab. Health Records Group	• ePEX Governance Group • SystmOne Strategy Group	• Corporate Records Group