focus
independent adult social work

Information Governance Management Framework & Strategy

Heritage House, Fisherman's Wharf, Grimsby, DN31 1SY

Contents

Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within focus Independent Adult Social Work C.I.C and its associated partner organisations and the Integrated Urgent Care (IUC) Alliance IGMF.

Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

The Data Security & Protection Toolkit DSPT is an online tool that enables organisations to measure their performance against the information governance requirements and compliance with the toolkit provides assurance that organisations have established good practice around the handling of information, are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

Information Governance Strategy

The development of this IG Framework will support an IG Strategy which you can find within Appendix B – which is in operation for focus.

Aim

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that high standards of IG are maintained. This Information Governance Management Framework is based on, and adheres to, the focus C.I.C – Information Security Policy.

Partner organisations are responsible for ensuring that commensurate policies, procedures and guidelines are in place within their own organisations and that individuals employed by them understand their obligations as detailed within them.

Data Security & Protection Toolkit (DSPT)

Completion of the DSPT is mandatory for all organisations connected to N3 the proprietary NHS computer network, for organisations using NHS Mail and providing NHS services. All organisations are required to score on all requirements at level 2 or 3 to be at a satisfactory level. Annual plans will be developed year on year from the DSPT to achieve a satisfactory level in all requirements. As the DSPT is a publicly available assessment the scores of

partner organisations will be used to assess their suitability to share information and to conduct business with.

Caldicott Guardian

The Caldicott Guardian for focus C.I.C is the Chief Executive Officer (CEO).

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate and secure information-sharing.

The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

Senior Information Risk Owner (SIRO)

The SIRO for focus C.I.C is the Head of Business & Governance

The SIRO is an Executive Director or Senior Manager/Leader who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk for the focus Board and provide written advice to the CEO in regard to information risk.

The SIRO must understand how the strategic business goals of the organisation and how other organisations' business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the organisation and advises the focus Board on the effectiveness of information risk management across the Organisation. This work is supported by Information Asset Owners (IAO) within departments who manage risks to specific systems and feed this information to the SIRO.

Data Protection Officer (DPO)

The DPO for focus C.I.C is the Head of Information & Security.

The DPO is an Executive Director or Senior Manager/Leader who will take overall ownership of the Organisation's Information Governance Management Framework, act as champion for information governance and security for the focus Board and provide written advice to the CEO in regard to information governance.

The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within focus C.I.C. This role includes but is not limited to: -

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures;
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties;
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance; and
- providing a focal point for the resolution and/or discussion of IG issues.

Managers/Leaders

Managers/Leaders are responsible for ensuring that their staff, both permanent and temporary, are aware of:

- all information security policies and guidance and their responsibility to comply with them;
- their personal responsibilities for information security;
- where to access advice on matters relating to security and confidentiality; and
- the security of their physical environments where information is processed or stored.

Staff

Individual employees have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

Data Protection Act (DPA)

The Data Protection Act is the most fundamental piece of legislation that underpins Information Governance. focus C.I.C are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for Privacy Impact Assessments (PIA) are highlighted these will be completed.

The Data Protection Principles are detailed at Appendix C.

General Data Protection Regulations (GDPR)

The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. focus C.I.C is a processor, therefore GDPR places specific legal obligations on focus C.I.C; for example, focus C.I.C is required to maintain records of personal data and processing activities. focus C.I.C has legal liability for a breach. The GDPR applies to processing carried out by organisations operating within the EU. The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Law Enforcement Directive (LED)

The EU Data Protection Directive 2016/680, also known as the Law Enforcement Directive (LED), complements the General Data Protection Regulation (GDPR).

It sets out the requirements for:

- the processing of personal data for criminal law enforcement purposes;
- the free movement of such data; and
- replaces the 2008 Council Framework Decision (2008/977/JHA) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The Directive applies to EU Member States (including the UK), Part 3 of the Data Protection Bill 2017 intends to implement the EU Law Enforcement Directive into domestic UK law.

Caldecott Principles and Requirements

The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013, have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

Government Response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly.

The Caldicott Principles are detailed at Appendix E.

Handling Confidential Information

When handling confidential information and especially where an individual can be identified from the information to be processed, the organisation must ensure that it has determined and documented a legal basis for processing that information.

For more detailed guidance please refer to the focus C.I.C – Confidentiality Policy

Privacy Impact Assessments

All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements. A PIA form will be undertaken for each.

Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. focus C.I.C are committed to a robust risk assessment process by Information Asset Owners.

For more detailed guidance please refer to the focus C.I.C – Information Governance Policy – Section 3.3.

Third Party Contracts

The organisation will ensure that contracts with third parties providing services to and on behalf of focus C.I.C or its clients include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that Contractors are aware of their IG obligations.

Training and Guidance

focus C.I.C recognises the importance of educating staff on their responsibilities and best practice on security and management of information. All focus C.I.C employed staff will be required to complete information governance training

The NHS ESR training system will be used for mandatory and statutory training to provide a consistent message to staff. There are training requirements specific to the roles discussed above which will need to be completed through the Information Governance Training Tool website (IGTT). Within the IGTT there are specific modules available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the modules relevant to their roles.

Incident Management and Investigation

Incidents must be reported and managed through the Incident Reporting Procedure. The Central Business Unit will have an active involvement in all IG related incidents to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature will be reported to the SIRO.

For more detailed guidance please refer to the Serious/Incident Reporting Process.

Where incidents occur within a partner organisation carrying out work under the focus C.I.C brand these should be reported and investigated using internal procedures of the organisation. Upon logging of the incident the focus C.I.C SIRO should be made aware to allow risks and service delivery issues to be assessed.

Reference Material

Internal

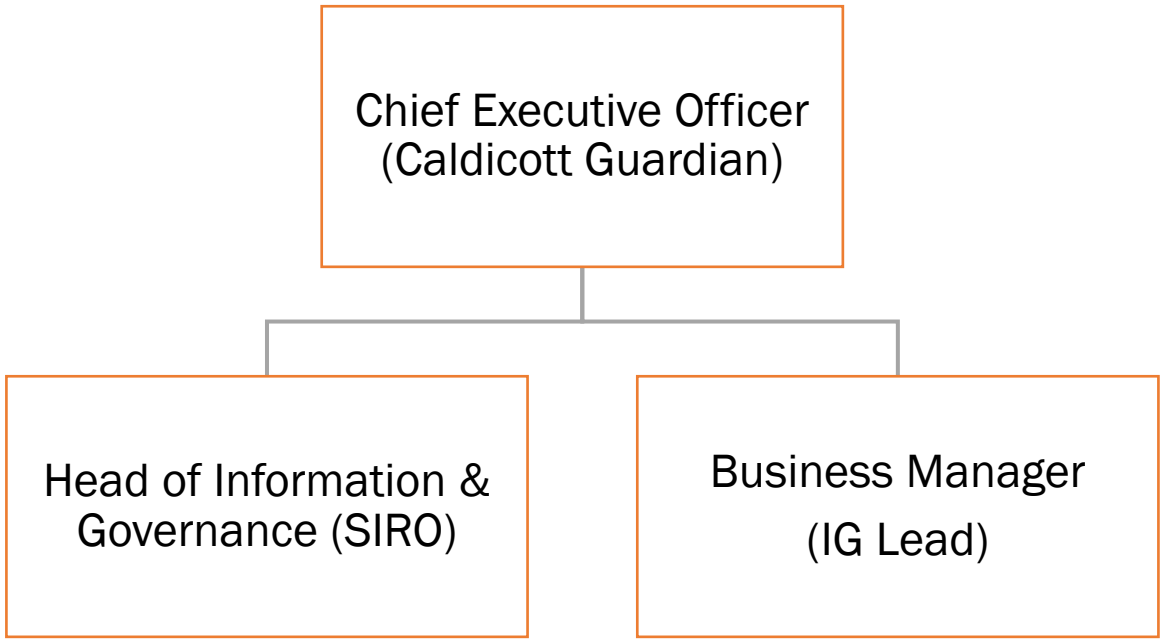
- Information Governance Policy
- Information Security Policy
- Data Protection Policy
- Records Management & Data Quality policy
- Major IT Incident Guidance & Protocol
- Confidentiality Policy
- Subject Access Request Process
- Privacy Impact Assessment Policy
- Internal Emergency Procedure and Response Plan
- External Emergency Procedure and Response Plan
- focus Case Recording Policy
- focus Agile Policy
- focus Code of Conduct
- Incident Reporting Process
- Serious Incident Reporting Policy
- Systems Development Access and Data Request Protocol
- Framework for responsible reporting

All of these documents are available on the Intranet site.

External

- Care Act 2014
- Data Protection Act 1998
- Human Rights Act 1998 (Specifically Article 8)
- NHS Information Governance*:* Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013.
- HSCIC: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- HSCIC: A guide to confidentiality in health and social care: references - September 2013
- National Information Board and DH: Personalised Health and Care 2020
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice

Appendix A – Organisational Structures



Appendix B – Information Governance Strategy 2017- 2019

1. The IG Strategy will be based upon a vision of a long term delivery of clear open principles to ensure that:

   1.1. That focus C.I.C organisation complies with all statutory requirements

   1.2. That focus C.I.C organisation has an information governance strategy that supports the achievement of corporate objectives

   1.3. That focus C.I.C organisation can demonstrate an effective framework for managing information governance assurance

   1.4. Staff are aware of their responsibilities and the importance of information governance

   1.5. Information governance becomes a systematic, efficient and effective part of business as usual for the organisation

   1.6. Information governance is integrated into the change control process

   1.7. That there are effective methods for seeking assurance across the organisation and with its key partners

   1.8. That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequate

Appendix C – Data Protection Principles

1. 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.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix D – Caldecott Principles

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data 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).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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.