

Information Governance Policy - Template

Information Governance Policy

1. Summary

1.1. Information is a vital asset, both in terms of the clinical management of individual service users and the efficient management of services and resources. It plays a key part in clinical governance, service planning, performance management and compliance with Care Quality Commission (CQC) regulations.

1.2. It is of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

2.1. **[Insert organisation name]** (hereafter referred to as "us", "we", or "our") recognises the need for an appropriate balance between openness and confidentiality in the management and use of information *i.e.* Information Governance (IG).

2.2. The importance of safeguarding both personal information about service users and staff and commercially sensitive information is paramount; however, we emphasise the importance of sharing service user information with other Health & Social Care organisations and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest. In all instances, the focus remains on the safeguarding and sharing of personal, sensitive and confidential information in line with legal and regulatory requirements.

2.3. We believe that accurate, timely and relevant information is essential to deliver the highest quality Health & Social Care. As such it is the responsibility of all staff and managers to ensure and promote the quality of information and to actively use information in decision making processes.

3. Our approach to Information Governance (IG):

3.1. We undertake to implement IG effectively and will ensure the following:

- i. Information will be protected against unauthorised access;
- ii. Confidentiality of information will be assured;
- iii. Integrity of information will be maintained;
- iv. Information will be supported by the highest quality data;
- v. Regulatory and legislative requirements will be met;
- vi. Business continuity plans will be produced, maintained and tested;
- vii. IG training will be available to all staff as necessary to their role;
- viii. All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4. Procedures.

[The procedures & policies may have different names in your organisation.

You should update the following to reflect this.]

4.1. This IG policy is underpinned by the following policies and procedures:

- i. Record Keeping policy & procedure **[Insert Policy Number]** that set out how service user records will be created, used, stored and disposed of;
- ii. Access policy & procedure [Insert Policy Number] that sets out procedures for the management of access to confidential information;

[Note that this policy should cover hard-copy (paper) based information and, if applicable in your organisation, digital information.]

- iii. Monitoring of Business Communications policy & procedure [**Insert Policy Number**] that sets out procedures around the transfer of confidential information;
- iv. Data Security Breach policy & procedure [**Insert Policy Number**] that sets out the procedures for managing and reporting information incidents;
- v. Business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer systems;
- vi. Staff Confidentiality Code of Conduct [**Insert policy number**] that provides staff with clear guidance on the disclosure of personal information.

4.2. There are 4 key interlinked strands to the IG policy:

- i. Openness
- ii. Legal compliance
- iii. Information security
- iv. Quality assurance

5. Openness

5.1. We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our responsibilities as outlined in the Health and Social Care Act 2008 (Regulated Activities), Regulations 2014: Regulation 20: Duty of candour.

5.2. Service users should have ready access to information relating to their own health care, their options for treatment and their rights as service users.

5.3. There are clear procedures and arrangements for handling queries from service users and the public.

5.4. There are clear procedures and arrangements for liaison with the press and broadcasting media.

6. Legal Compliance

6.1. All identifiable personal information relating to service users is confidential.

6.2. All identifiable personal information relating to staff is confidential except where national policy on accountability and openness requires otherwise.

6.3. We will establish and maintain policies to ensure compliance with the Data Protection Act 1998, Human Rights Act 1998 and the Common Law Duty of Confidentiality.

6.4. We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998, etc.).

6.5. We will undertake or commission annual assessments and audits of our compliance with legal requirements.

7. Information Security

7.1. We will establish and maintain policies for the effective and secure management of its information assets and resources.

7.2. We will undertake or commission annual assessments and audits of our information arrangements.

7.3. We will promote effective confidentiality, security and information sharing practices to our staff through policies, procedures and training.

7.4. We will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

8. Information Quality Assurance

8.1. We will establish and maintain policies and procedures for information quality assurance and the effective management of records.

8.2. We will undertake or commission annual assessments and audits of our information quality and records management arrangements.

8.3. Senior staff are expected to take ownership of, and seek to improve, the quality of information within our service.

8.4. Wherever possible, information quality should be assured at the point of collection. For example, when employing new staff all details taken should be thoroughly checked to ensure accuracy.

8.5. Data will be stored and recorded in line with Data Standards legislation – *i.e.* the Data Protection Act 1998.

8.6. We will promote information quality and effective records management through policies, procedures/user manuals and training.

9. Responsibilities

9.1. The designated Information Governance Lead for the organisation is **[insert IG Lead name here]** and, in their absence, their Deputy **[Insert Deputy Name Here, if applicable]**.

The key responsibilities of the lead are:

- i. To define **[insert organisation name]**'s policy in respect of IG and ensuring that sufficient resources are provided to support the requirements of the policy.

- ii. To complete the NHS Information Governance Toolkit and maintain compliance *i.e.* Level 2 or above in all requirements.
- iii. Developing and implementing IG procedures and processes for the organisation; **[those required to complete the IG Toolkit have been provided for you]**
- iv. Raising awareness and providing advice and guidelines about IG to all staff;
- v. Ensuring that any training made available is taken up;
- vi. Coordinating the activities of any other staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- vii. Ensuring that service user data is kept secure and accurate and that all data flows, internal and external, comply with the Caldicott Principles;
- viii. Monitoring information handling in the organisation to ensure compliance with law, guidance and the organisation's procedures;
- ix. Ensuring service users are appropriately informed about the organisation's information handling activities;
- x. Overseeing changes to systems and processes;
- xi. Incident reporting. Any/all breaches will be appropriately dealt with, investigated and reported to NHS Digital via the IG Toolkit website (<https://www.igt.hscic.gov.uk/>).
- xii. Ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS Information Governance assurance framework.

[You need to state who is responsible for the following within your organisation, if they are not applicable then please delete.]

9.2. **[insert job title here]**, is responsible for the Information Assets Register – this is the list of all devices and computer equipment in the organisation including who is responsible for it and what security has been applied to it, *i.e.* passwords or encryption, it also contains storage areas and protections for non-digital records.

9.3. **[insert job title here]**, is responsible for monitoring and enforcing compliance with the terms and conditions of NHS Smartcard usage (the Registration Authority manager).

9.4. **[insert job title here]**, is responsible for reviewing transfers of personal information outside of the UK. **[Note that if this is applicable it may be the responsibility of the same person who maintains the IAR].**

9.5. **[insert job title here]**, is responsible for the ICT services including access rights to computer based systems.

9.6. All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

10. Policy Approval

10.1. **[Insert organisation name]** acknowledges that information is a valuable asset, therefore it is wholly in our interest to ensure that the information we hold, in whatever form, is appropriately governed, protecting the interest of all stakeholders.

10.2. This policy, and its supporting standards and work instruction, are fully endorsed by **[insert either the Board or Senior Management of your organisation]** through the production of these documents and their minuted approval.

10.3. All staff, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of **[insert organisation name]**'s objectives and the delivery of effective healthcare to the service users.

10.4. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

