Information Governance Policy Framework

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Arch Health CIC.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Arch Health CIC.

B. Document Details

Classification:	Data Security & Protection
Lead Director:	Dr Tim Worthley, Clinical Lead
Organisation:	Arch Health CIC
Document Reference:	Information Governance Policy Framework
Current Version Number:	V1.1
Current Document Approved By:	Tim Worthley
Date Approved:	17.05.2018
Ratified by Arch Board:	22.05.2018
Renewal Due Date:	01.05.2019

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.1	17.5.8	PS	TW	Note: in need of a large review post guidance re DPST in the NY

Summary

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.

It is therefore 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.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in modern healthcare delivery. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information governance management
- Clinical information assurance to ensure safe patient care
- Confidentiality and data protection assurance
- Information security assurance
- Secondary use assurance

1. Principles

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. As such, it is the responsibility of everyone in the Practice to ensure and promote the quality of information and to actively use information in decision making processes.

The aim of this document is to:

- Ensure that data is:
    - Held securely and confidentially
    - Obtained fairly and lawfully
    - Recorded accurately and reliably
    - Used effectively and ethically
    - Shared and disclosed appropriately and lawfully
- Protect information assets from threats, whether internal or external, deliberate or accidental. Arch Health CIC will ensure:
    - Information will be protected against unauthorised access
    - Confidentiality of information will be assured
    - Integrity of information will be maintained
    - Information will be supported by high quality data
    - Regulatory and legislative requirements will be met
    - Business continuity plans will be produced, maintained and tested
    - Information governance training will be available to all staff
    - All breaches of information security, actual or suspected, will be reported to and investigated by the Caldicott Guardian

2. Roles and responsibilities

2.1 Chief Executive

It is the role of the Chief Executive to define the Practice's policy in respect of Information Governance, taking into account legal and NHS requirements.

The Chief Executive is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

2.2 Practice Manager

The Practice Manager is the designated Information Governance Lead in the Practice and is responsible for:

- Overseeing day to day Information Governance issues;
- Developing and maintaining policies, standards, procedures and guidance;
- Coordinating Information Governance in the Practice;
- Carry out regular audit of Information Governance compliance;
- Raising awareness of Information Governance; and
- Ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines, including the development and delivery of training.

2.3 Caldicott Guardian

The Medical Director has been appointed the Caldicott Guardian at Arch Health CIC. The Caldicott Guardian is responsible for the establishment of procedures governing access to, and the use of patient-identifiable information and, where appropriate, the transfer of that information to other bodies. The Caldicott Guardian will work closely with the Chief Executive and Practice Manager:

- To develop and implement procedures to ensure that all routine uses of patient-identifiable data are identified and documented and that their use has been established as being justified.

- To develop and implement criteria and a process for dealing with ad-hoc requests for patient-identifiable patient data for non-clinical purposes.

- To establish Information Sharing Protocols to govern the use and sharing of patient-identifiable data between organisations both within and outside the NHS.

- To ensure standard procedures and protocols are in place to govern access to patient-identifiable data.

- To ensure standard procedures and protocols are in an understandable format and available to all staff

- Raise awareness through training and education to ensure that the standards of good practice and Caldicott principles are understood and adhered to.

- Advise project leads on all aspects of Caldicott, acting as an expert resource for them.

- To bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.

- To raise concerns about any inappropriate uses of patient-identifiable data with external bodies where necessary.

- On an annual basis, to participate in the Information Governance Toolkit Assessment

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health.

2.4 All staff

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day to day basis.

Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy/strategy and procedure manuals
- Line manager
- Training course and induction
- Mandatory refresher training
- Other communication methods, e.g. team meetings, clinical governance meetings, incident review.

Information governance training is required to be undertaken on an annual basis.

All staff must make sure that they use Arch Health CIC's IT systems appropriately, and adhere to relevant policies and procedures.

Staff must raise questions or concerns regarding information governance and related policies and procedures, including compliance and breach, with their line manager, the Practice Manager or the Caldicott Guardian.

3. Information Governance Policy Framework

Arch Health CIC's Information Governance Framework is supported by a set of policies and related procedures which cover all aspects of Information Governance and Information Governance toolkit requirements.

Key policies are:

Data security & protection policy	This policy sets out the roles and responsibilities for compliance with the Data Protection Act & GDPR
Freedom of Information policy	This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act.
Confidentiality policy	This policy lays down the principles for Arch Health CIC staff with access to personal or confidential business information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security in order to comply with obligations of confidentiality and the NHS Confidentiality Code of Practice.
Record keeping and management policy	This policy is to promote and support effective record-keeping and procedures for ensuring that

	legal requirements are adhered to.

The Arch Health CIC staff handbook includes an introduction to Information Governance and summarises key obligations of all staff.

4. Implementation of this policy

This document will be provided to all staff upon induction, and reviewed at mandatory refresher training.

Review of information governance compliance and breaches will form part of monthly Practice meetings, encouraging staff to identify areas for improvement or training needs.

Compliance with the policies and procedures described in this document will be monitored by the Chief Executive, Caldicott Guardian and Practice Manager, with annual audit and review of the policy. Monitoring and revision of the document will take place sooner in the event of legislative changes or a serious incident relating to information governance.