Information Governance and Data Protection Policy

Version Control

Reference Number IGP1	**Version** 5.0	**Status** Final	**Sponsor(s)/Author(s)** N Salkeld
Document objectives: Sets out PH's policy on how information governance plays a key part in supporting clinical governance, service planning and performance management.			
Intended Recipients: All staff			
Group/Persons Consulted: THIS			
Training/Resource Implications: Induction training, awareness of policy folder			
Approving Body and Date first approved		Executive Board – July 2012; ratified 28 May 2026	
Next Review Date		May 2029	

The table below logs the history of the steps in development of the document.

Version	Date	Author	Comment
1.0	July 2012	N Salkeld P Godbole	
2.0	Jan 2014	N Salkeld P Godbole	
3.0	Jan 2015	N Salkeld	None
4.0	Mar 2018	N Salkeld	Rewrite of policy
5.0	Mar 2021	N Salkeld	SIRO updated to JMM
6.0	May 2026	N Salkeld	Training course updated

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and in the management of services and resources. However, it is of paramount importance that any information relating to services, patients and employees is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

Pioneer Healthcare (PH) is fully committed to developing a robust governance framework for information management in line with national and legal requirements.

Information Governance aims to provide the framework which will enable PH to bring together all the initiatives aimed at meeting the requirements, standards and best practice that apply to the handling of personal information. This will necessitate the development, implementation and maintenance of systems and processes supported by appropriate policies, procedures and education, training, and development. Clear lines of individual responsibility and management accountability and structures will also need to be identified.

1.1 Purpose of the Policy

The purpose of the Information Governance policy is to demonstrate:

- Executive support and commitment to Information Governance;
- Executive support and commitment to the approach which PH plans to take to implementing Information Governance;
- Appropriate, visible and complete arrangements are in place in PH to deliver the Information Governance Framework.

1.2 Scope of the Policy

Information Governance standards apply to any information held, obtained, recorded, used or shared by PH that relates to personal information.

Personal or 'person identifiable' information refers to any information from which an individual, whether a patient, client, carer, or employee, can directly or indirectly be identified , such as name, date of birth, NHS number, address. All person identifiable information is regarded as confidential information. Sensitive personal data also contains information which could be seen as discriminatory. These are defined by the DPA 2018.

Certain information which may not be person identifiable but relate to PH and its services may be regarded as sensitive and as such be treated as confidential information e.g. commercially sensitive information.

Information Governance standards apply to confidential information stored and used on any type of media including for example, paper records, electronic records, video, audio, x-ray, digital images.

The specific areas of focus are covered in section 1.5 of this document.

1.3 Related PH Policies and Procedures

PH has a range of existing policies supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.

1.4 Information Governance and the NHS IG Toolkit

Clear standards for information handling based on current legislation and Government and National guidance have been set by the Department of Health. The Information Governance toolkit has been developed to enable NHS organisations to self-assess their compliance to these standards and implement year on year improvement plans to achieve and maintain compliance.

1.5 Information Governance Initiatives

Information Governance and the Information Governance toolkit currently encompass specific areas of focus called 'initiatives':

- Information Governance Management
- Secondary Uses Assurance
- Clinical Information Assurance
- Confidentiality & Data Protection Assurance
- Information Security Assurance
- Corporate Information Assurance

1.6 NHS Operating Framework

Requirements of the NHS Operating Framework 2010/11, sets a focus on sustaining robust Information Governance by:

- ensuring compliance at minimum level 2 performance for all NHS IG Toolkit standards;
- mandating all staff to complete annual basic IG training appropriate to their role through the national online NHS IG Training Tool or other Connecting for Health approved materials.
- continuing to report on the management of information risks in statements of internal controls and to include details of data loss and confidentiality breach incidents in annual reports;
- ensuring an IG audit utilising the centrally provided audit methodology is included within each organisation's auditors work plan.
- ensuring that relevant staff are aware of and trained to be able to use anonymised or pseudonymised data and ensuring appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of patient identifiable data.

2. Principles

PH recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. It fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality and security arrangements to safeguard both personal information about patients and staff and commercially sensitive information. PH 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.

Key to the principles of PH's Information Governance Policy is the provision of information explaining to patients and carers how their personal information is used and shared by PH.

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

There are 4 key interlinked principles for the use of information:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1 Openness

- Non-confidential information on PH and its services should be available to the public through a variety of media, in line with PH's code of openness
- PH will establish and maintain policies to ensure compliance with the Freedom of Information Act which will include compliance with the European Directive for environmental information
- PH will undertake or commission regular assessments and audits of its policies and arrangements for openness
- Patients will have ready access to information relating to their own health care, their options for treatment and their rights as patients
- PH will have clear procedures and arrangements for liaison with the press and broadcasting media
- PH will have clear procedures and arrangements for handling queries from patients and the public

2.2 Legal Compliance

- PH regards all personal information relating to patients as confidential except where mandated disclosure is required

- PH regards all personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise

- PH will undertake or commission regular assessments and audits of its compliance with legal requirements

- PH will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality

- PH will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation. Information Sharing Agreements will be developed with local partners to ensure compliance with the Data Protection Act 2018.

- PH will ensure compliance with the Data Protection Act 2018 prior to using or disclosing personal information, as well as common law obligations for personal information held in confidence requiring consent before disclosure to a third party, unless exceptional circumstances apply.

2.3 Information Security

- PH will establish and maintain policies for the effective and secure management of its information assets and resources and ensure transfers of information into and out of the organisation are legal and secure

- PH will undertake or commission regular assessments and audits of its information and IT security arrangements

- PH will promote effective confidentiality and security practice to its staff through policies, procedures and training

- PH will protect confidentiality of service user information through use of pseudonymisation and anonymisation techniques where appropriate

- PH will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

2.4 Information Quality Assurance

- PH will establish and maintain policies and procedures for information quality assurance and the effective management of records

- PH will undertake or commission regular assessments and audits of its information quality, including Clinical Coding and records management arrangements

- PH expects its Managers and clinicians to take ownership of, and seek to improve, the quality of information within their services

- Wherever possible, information quality will be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- PH will promote information quality and effective records management through policies, procedures/user manuals and training

3. Data Protection and UK GDPR Compliance

3.1 Commitment to Data Protection

Pioneer Healthcare Limited recognises the importance of protecting personal information and is committed to ensuring that all personal data is processed lawfully, fairly and transparently in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated legislation.

Pioneer Healthcare Limited will ensure that personal information relating to patients, staff, contractors, suppliers and other stakeholders is handled securely and only used for legitimate organisational purposes.

3.2 Data Protection Principles

Pioneer Healthcare Limited will ensure that all personal data is:

a) Processed lawfully, fairly and transparently

Personal information will only be processed where there is a lawful basis to do so and individuals will be informed about how their information is used.

b) Collected for specified, explicit and legitimate purposes

Personal data will only be collected for defined purposes and will not be processed in ways incompatible with those purposes.

c) Adequate, relevant and limited to what is necessary

Only the minimum amount of information necessary to fulfil the intended purpose will be collected and processed.

d) Accurate and kept up to date

Reasonable steps will be taken to ensure personal information is accurate, complete and corrected where inaccuracies are identified.

e) Retained only for as long as necessary

Personal information will be retained in accordance with the NHS Records Management Code of Practice and Pioneer's Records Retention Schedule.

f) Processed securely

Appropriate technical and organisational measures will be implemented to protect information against unauthorised access, accidental loss, destruction or damage.

g) Accountable

Pioneer Healthcare Limited will be able to demonstrate compliance with UK GDPR requirements through appropriate governance, policies, training and assurance arrangements.

3.3 Lawful Basis for Processing

Pioneer Healthcare Limited processes personal information under the lawful bases provided by UK GDPR and the Data Protection Act 2018.

For healthcare activities this will commonly include:

- Performance of a contract;
- Compliance with legal obligations;
- Performance of tasks carried out in the public interest;
- Provision of health or social care services;
- Legitimate organisational interests where appropriate.

Special category data, including health information, will only be processed where an additional condition for processing under Article 9 UK GDPR applies.

3.4 Data Subject Rights

Individuals whose personal data is processed by Pioneer Healthcare Limited have rights under UK GDPR including:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure where applicable;
- The right to restrict processing;
- The right to object to processing;
- The right to data portability where applicable;
- Rights relating to automated decision making and profiling.

Pioneer Healthcare Limited will ensure appropriate arrangements are in place to facilitate these rights in accordance with statutory timescales.

3.5 Subject Access Requests

Individuals have the right to request access to personal information held about them by Pioneer Healthcare Limited.

Requests for access to personal data will be managed in accordance with UK GDPR requirements and will normally be responded to within one calendar month of receipt of a valid request and confirmation of identity.

Where requests are complex or numerous, Pioneer Healthcare Limited may extend the response period in accordance with legislation and will inform the requester accordingly.

3.6 Data Protection Impact Assessments

Pioneer Healthcare Limited will undertake Data Protection Impact Assessments (DPIAs) where processing activities are likely to result in a high risk to the rights and freedoms of individuals.

Examples include:

- Introduction of new technologies;
- New systems containing personal information;
- Large-scale processing of special category data;
- Significant changes to existing processing arrangements.

DPIAs will be undertaken at an early stage of project development to ensure privacy risks are identified and mitigated appropriately.

3.7 Personal Data Breaches

Any actual or suspected personal data breach must be reported immediately in accordance with Pioneer's Incident Management Policy and Information Security arrangements.

All reported incidents will be investigated and assessed to determine:

- The nature of the breach;
- The sensitivity of the information involved;
- The number of individuals affected;
- The potential impact on affected individuals;
- Whether notification to the Information Commissioner's Office is required.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, Pioneer Healthcare Limited will notify the Information Commissioner's Office within 72 hours of becoming aware of the breach, in accordance with UK GDPR requirements.

3.8 Records Retention and Secure Disposal

Pioneer Healthcare Limited will retain records in accordance with the NHS Records Management Code of Practice and applicable statutory retention requirements.

When records are no longer required, they will be securely destroyed using approved methods appropriate to the sensitivity of the information.

Electronic records will be securely deleted and paper records confidentially destroyed in accordance with organisational procedures.

3.9 International Transfers of Personal Data

Pioneer Healthcare Limited will ensure that personal information is not transferred outside the United Kingdom unless appropriate safeguards are in place and such transfers comply with UK GDPR requirements.

Where cloud-based systems or third-party providers are utilised, Pioneer Healthcare Limited will ensure that appropriate contractual and security arrangements are in place to protect personal information.

3.10 Accountability and Assurance

Pioneer Healthcare Limited will maintain appropriate governance arrangements to demonstrate compliance with information governance and data protection requirements including:

- Annual Data Security and Protection Toolkit submissions;
- Mandatory staff training;
- Information Governance audits;
- Incident reporting and learning;
- Regular policy review;
- Board oversight of information risks.

4. Responsibilities

4.1 Corporate Management Structures

4.1.1 Pioneer Healthcare Board

PH Board has overall accountability for PH's ability to meet the Information Governance requirements. The Board is responsible for:

- Receiving, considering and approving regular Information Governance reports and briefings

- Signing off PH's Information Governance Strategy and annual Information Governance toolkit central returns

4.1.2 Executive Management Group/Risk Management Committee

On behalf of PH Board, the Executive Management Group/Risk Management Committee is responsible for ensuring adequate Information Governance arrangements are in place. Responsibilities include:

- Ensuring the Information Governance Strategy is in line with the overall strategic ambition, goals and objectives of PH

- Ensuring effective management structures, work programmes and policies are in place to deliver the Information Governance agenda

- Understanding key elements of the IG strategy and the risks and implications associated with failure to meet requirements

- Ensuring that sufficient resources are provided to support implementation of PH Information Governance Framework, performance monitoring outcomes of improvement plans and addressing the risks of non-compliance

4.1.3 Information Governance Committee

The Information Governance Committee is responsible on behalf of the Executive Management Group for

- Developing, implementing and maintaining Information Governance policies and associated Information Governance Framework to provide assurance to PH Board through the Executive management Group, that effective arrangements are in place

- Over-seeing and monitoring PH annual assessments; and monitoring progress against agreed strategy, policy and improvement plans

- Informing the review of the organisation's management and accountability arrangements for Information Governance, undertaking or commissioning regular audits and review of the strategy, management arrangements, policies and processes

- Agreeing Information Governance relevant reports and recommendations and timely preparation of the annual Information Governance assessment for PH Board sign off

- Working with Clinical, Corporate and Support Services to promote and embed Information Governance into the organisational culture

Specific Information Governance Senior Management Roles

4.1.4 Information Governance Executive Lead

PH Executive Lead has board level responsibilities for Information Governance and enables a direct reporting line to PH Board. It is the executive leads responsibility alongside the Information Governance Committee, to direct the management of PH Information Governance Framework.

4.1.5 Caldicott Guardian

PH Caldicott Guardian has board level responsibilities for PH's Caldicott Function and enables a direct reporting line to PH Board and the Governance Committee. The Caldicott Guardian is responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing.

4.1.6 Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) has board level responsibilities and takes overall ownership of PH's Information Risk and Information Asset Management processes. The SIRO provides written advice to the Accounting Officer on the content of PH's Statement of Internal Control in regard to information risk and reports information incidents in the Annual Report.

4.1.7 Data Controller

The Data Controller determines the purposes for which, and the manner in which, personal information is to be processed in PH with responsibility for ensuring PH is registered and compliant with the Data Protection Act 2018. They must 'Notify' PH activities with the Information Commissioner's Office.

4.1.8 Freedom of Information Lead

The Freedom of Information (FoI) Lead is a senior management level lead who ensures organisational procedures and processes are in place to comply with the FoI Act. The Public Authority's compliance with the Freedom of Information Act and for reporting Freedom of Information issues to PH Board (or equivalent) is a delegated responsibility from the Chief Executive to the appropriate Director to act as PH Freedom of Information lead.

Other Associated Senior Management Roles

4.1.9 Managing Director

The MD provides an organisational statement that Terms and conditions of Employment on all current and new employment contracts contain comprehensive information governance compliance requirements.

Other Specific Information Governance Management Roles

4.1.10 Information Governance Operational Lead

PH Information Governance Lead has responsibility for managing the overall co-ordination, publicising and monitoring of PH Information Governance Framework. PH IG lead has specific responsibility for the development of the IG strategy and policy, producing routine performance monitoring reports and producing IG toolkit central returns on behalf of PH.

4.1.11 Information Asset Owners

Lead managers with assigned Information Asset Ownership have responsibilities to provide the SIRO with assurance that information security has been properly considered and addressed within the design, development, implementation, operation and decommissioning stages of an asset's lifecycle.

4.1.12 Contract Directors

Responsibility for the application of Information Governance Agreements as part of contractual arrangements with 3rd Parties rests with the Director (s) who is/are responsible for the relevant third party Service Level Agreement or Supplier/Service Contract.

Operational Management Responsibilities & Structures

4.1.13 Managers

All Department Managers are responsible for ensuring that Information Governance related policies and supporting standards and guidelines are built into local processes and that there is on-going compliance within their teams.

Managers are required to support the implementation of PH Information Governance Strategy at a local operational level. They have responsibility for ensuring that their teams undertake available training and are kept up to date regularly through access to policy bulletins and other key PH communications relating to Information Governance.

4.1.14 Employees & staff working on behalf of PH

All individual PH employees, whether permanent, temporary or contracted through 3rd party agencies such as students, agency staff or contractors, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All employees are required to undertake annual mandatory training in Information Governance as appropriate to their role to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance.

5. Information Governance Training and Induction

To ensure organisational compliance with the law and central guidelines relating to Information Governance staff must receive appropriate training. Therefore, IG training is mandatory for all staff, and training needs routinely assessed, monitored and adequately provided for.

5.1 Compulsory Basic Annual Information Governance Training

All staff - permanent or on temporary contracts of more than 3 months (including students, trainees and agency staff and contractors) must complete basic annual Data Security & Awareness (or Information Governance equivalent) training.

5.2 Additional Role Based Information Governance Training

Additional role based Information Governance Training will be mandated as identified through a role base analysis or national and local policy changes.

6. Information Governance Policies & Procedures

6.1 Policy Audit and Review

This and other IG policies are subject to regular audit and review to monitor effectiveness and compliance. Audit feedback and results of spot checks will be used to review and revise the policy to ensure that it is kept up to date and in line with national guidelines.

6.2 Failure to Comply with Policy

Failure to comply with the IG policy and other related policies and procedures may be regarded as a disciplinary offence. Where relevant PH Disciplinary Policy and

Procedure will be invoked to manage Information Governance breaches and the consequence of staff misconduct may result in dismissal. Legal action may be taken where a criminal offence is found to have been committed.

7. Information Governance Policy Approval

Pioneer Healthcare acknowledges that information is a valuable asset, therefore it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

This policy is fully endorsed and approved by PH Board.

Appendix 1

Information Governance Management Arrangements

Information Governance Executive Lead: Medical Director – John McMullan
Senior Information Risk Officer Medical Director – John McMullan
Data Controller (Data Protection Act): Chief Executive Officer – Prasad Godbole
Caldicott Guardian: Medical Director – John McMullan
Freedom of Information Lead: Medical Director – John McMullan
Information Governance Operational Lead: Director of Operations – Nicola Salkeld