Information Governance/Caldicott Guardian Policy

Document Control

A. Confidentiality Notice

This document and the information contained therein are the property of Dr Valda Porcionato Ltd ("the Organisation").

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 prior consent in writing from Dr Valda Porcionato Ltd.

B. Document Details

Organisation:	Dr Valda Porcionato Ltd
Current Version Number:	2.0
Date Approved:	23/03/2024
Review Date	23/03/2025

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.0	23/03/2023	Valda Porcionato	Valda Porcionato	
2,0	23/03/2024	Valda Porcionat	Valda Porcionat	

Information Governance/Caldicott Guardian Policy

1. 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

2. Principles

The Organisation recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Organisation fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

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.

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

There are 4 key interlinked strands to the Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

a) **Openness**

- Non-confidential information about the Organisation and its services will be available to the public through a variety of media, in line with the Organisation's code of openness.
- The Organisation undertakes or commission annual assessments and audits of its policies and arrangements for openness.
- Patients have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Organisation has clear procedures and arrangements for liaison with the press and broadcasting media.
- The Organisation has clear procedures and arrangements for handling queries from patients and the public.

b) Legal Compliance

- The Organisation regards all person identifiable information, including that relating to patients as confidential.
- The Organisation undertakes or commission annual assessments and audits of its compliance with legal requirements.
- The Organisation regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Organisation establishes 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).

c) Information Security

- The Organisation undertakes or commission annual assessments and audits of its information and IT security arrangements.
- The Organisation promotes effective confidentiality and security practice to its staff through policies, procedures and training.
- The Organisation establishes and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

d) Information Quality Assurance

- The Organisation undertakes or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- The Organisation promotes information quality and effective records management through policies, procedures/user manuals and training.

3. Responsibilities

It is the role of the Caldicott Guardian/Data Protection Officer [Romulo Rebelo] to define the Organisation's policy in respect of Information Governance, taking into account legal and requirements.

The Data Protection Officer is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

The Data Protection Officer is the designated Information Governance Lead in the Organisation and is responsible for:

- Overseeing day to day Information Governance issues;
- Developing and maintaining policies, standards, procedures and guidance;
- Coordinating Information Governance in the Organisation;
- Raising awareness of Information Governance; and
- Ensuring that there is on-going compliance with the policy and its supporting standards and guidelines.

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.

4. Policy Approval

The Organisation 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.

The Organisation will, therefore, ensure that all staff, contractors and other relevant parties observe this policy, in order to ensure compliance with Information Governance and contribute to the achievement of the Primary Care objectives and delivery of effective healthcare to the local population.

5. Caldicott Guardian/Data Protection Officer

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

5.2 Person identifiable information takes many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.
The Organisation must safeguard the integrity, confidentiality, and availability of sensitive information.

5.3 No one from the Organisation (this includes staff employed by commercial partners and volunteer groups) is allowed to share any person identifiable information unless it has been authorised by the Organisation's Caldicott Guardian. It is unlikely that this authorisation will be granted unless the access is on a need to know basis and justifiable against the Caldicott principles.

5.4 The Caldicott standard is based around six principles:

5.4.1 Justify the purpose-
Every purposed use or transfer of person identifiable information within or from an organisation should be clearly defined and scrutinised with continuing uses regularly reviewed by the Caldicott Guardian.

5.4.2 Don't use personal identifiable information unless it is absolutely necessary
- Person identifiable information items shall not be used unless there is no alternative.

5.4.3 Use the minimum necessary personal identifiable information
- Where use of person identifiable information is considered to be essential, each individual item of person information should be justified with the aim of reducing identity.

5.4.4 Access to personal identifiable information should be on a strict need to know basis
- Only those individuals who need access to person identifiable information should have access to it and they should only have access to the personal information items that they need to see.

5.4.5 Everyone should be aware of their responsibilities
- Actions should be taken to ensure that all staff who handle person identifiable information are aware of their responsibilities and obligations to respect confidentiality.

5.4.6 Understand and comply with the Law
- Every use of person identifiable information must be lawful. Individuals have a right to believe that personal information given in confidence will be used for the purposes for which it was originally given, and not released to others without their informed consent.