5 Coles Lane, Cambridge, UK, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org
www.optimumpatientcare.org

Policy Number: POL 2000
Version Number: 5.0
Effective Date: 20 FEB 2020
Review Date: 20 FEB 2021

INFORMATION GOVERNANCE POLICY

V5.0 20 FEB 2020

This is a Controlled Document. This policy is issued by the Company. Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Human Resources Department and/or appropriate delegate should ensure the policy is communicated to all staff and contractors where applicable. The master copy of this document is kept on the Company Policies and SOPs Smartsheet and NAS drive. A copy may be made available on the Company website for public transparency. Staff may print this document for training and reference purposes but are responsible for regularly checking for more recent versions of the document.

AUTHORS

Name: Francis K. Appiagyei

Position: Clinical Manager / IG Lead

AUTHORISATION

Name: Chris Price

Position: Commercial and Legal Director / SIRO

Signature: 

Date: 20 February 2020

CONTENT

ABBREVIATIONS

OPC or OPC UK	Optimum Patient Care Limited
POL	Policy
SOP	Standard Operating Procedure
HR	Human Resources
GP	General Practice
NHS	National Health Service
IG	Information Governance
DSP	Data security and protection
DSPT	Data Security and Protection Toolkit
GDPR	EU General Data Protection Regulation 2016
DPA	Data Protection Act 2018
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
SIRO	Senior Information Risk Owner
IAO	Information Asset Owner
ISM	Information Security Manager
ICO	Information Commissioner's Office

BACKGROUND

Optimum Patient Care Ltd (OPC) or referred to as 'Company', supports GP practices, commissioners, health researchers and the wider NHS to improve healthcare provision to patients and better patient outcomes. This policy is important because it will help people who work for the Company to understand how to handle and protect information for work and service provision.

PURPOSE

To provide guidance to staff and contractors on information governance (IG) with focus on data security and protection. This encompasses other related policies including Data Protection, Confidentiality, Information Security, Document and Records Management, Data Quality, etc. This policy provides a framework for handling information in a lawful and secure manner to appropriate ethical and quality standards.

The aims of this policy are:

1. To secure and protect the value of Company information assets by ensuring 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

2. To protect the Company information assets from threats, whether internal or external, deliberate or accidental, by ensuring:

- Information is protected against unauthorised access
- Confidentiality of information is assured where applicable
- Integrity of information is maintained
- Regulatory and legislative requirements are met and adhered to
- Data security and protection training is made available to staff and contractors
- Information incidents and data protection breaches are reported appropriately
- Business continuity plans are produced, maintained and tested

APPLICABILITY

This policy applies to Company staff, and associated persons such as secondees, third party and freelance contractors. Compliance with this policy is a legal and contractual duty for staff and contractors. Failure to comply with this policy may lead to disciplinary and/or legal action.

This policy applies to all forms of information, including but not limited to:

- paper and electronic filing systems;
- communications, including those sent by post, electronic mail, text messaging;
- information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device;
- information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internal or externally to a third party.

RESPONSIBILITY

All Employees:

- It is the responsibility of each employee to adhere to the policy.
- All employees must undertake the recommended annual data security and protection training.
- All employees must ensure they use the Company's information systems appropriately according to the relevant policies and procedures.
- All employees must report any incident involving a breach or suspected breach of the GPA and DPA to their line manager immediately.

Line Managers:

- Ensure policies relating to data security and protection are adhered to within their team and that there is on-going compliance.
- Ensure staff will receive instruction and direction regarding the policy from a number of sources:
    - policy/strategy and procedure manuals;
    - line manager;
    - specific training course; o other communication methods, for example, team meetings; and staff Intranet.
- Ensure any breaches of the policy are reported, investigated and acted upon via the appropriate reporting procedure.
- Support management and HR in monitoring and auditing of IG requirements.

Senior Management:

- Overall responsibility for strategic management, including ensuring that the Company policies are available and comply with legal, regulatory and good practice guidance requirements.
- Ensure appointments are in place to implement, monitor and improve data security and protection at the Company.
- Ensure data protection clauses are included in employment and contractor's contracts.

Caldicott Guardian (CG):

The Caldicott Guardian (CG) is a senior manager responsible for advising and advocating for the protection of Confidentiality at the Company in relation to people's healthcare information; to make sure such information is used lawfully, and patient confidentiality is upheld. The key responsibilities of the CG (**currently Victoria Carter**):

- Ensuring that the Caldicott Principles are respected at the Company when dealing with personal or confidential information.
- Ensuring that OPC satisfies the highest practical standards for handling personal or confidential information.
- Providing advice on options for lawful and ethical processing and sharing of information in relation to disclosures of personal or confidential information.
- Facilitating and enabling appropriate information sharing and approving information sharing decisions on behalf of the Company.
- Ensuring that confidentiality issues are appropriately reflected at Company board level and in Company strategies, policies and working procedures for staff.
- Oversee all arrangements, protocols and procedures where confidential information may be shared with external bodies both within, and outside, OPC.

Senior Information Risk Owner (SIRO):

The SIRO is a senior manager or director appointed to oversee information security and risk management of the Company's information assets. The key responsibilities of the SIRO (**currently Chris Price**):

- Oversee the development and implementation of strategies and policies to manage information risks within the existing information governance (IG) framework.
- Ensure the Company's approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff.
- Ensure effective systems are in place for staff awareness on the importance data protection and security; and staff receive appropriate training.
- Review annual information risk assessments, IG improvement plans and endorse actions to address identified risks and make improvements.
- Ensure there is a focal point for the resolution and / or discussion of information risk issues.
- Ensure Information Assert Owners (IAOs) are appointed to manage the Company's information assets.
- Ensure the Company board is adequately briefed on information risk issues and advise the board on the effectiveness of information risk management across OPC.
- Receive training as necessary to ensure he remain effectives in his role as SIRO.

Information Governance (IG) Lead:

The IG Lead is a senior manager appointed to act as the overall lead on IG work and improvements at the Company. The IG Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key responsibilities of the IG Lead (**currently Francis Appiagyei**):

- Support the SIRO in implementing information security for Company information assets.
- Develop and maintain comprehensive and appropriate documentation (responsibilities, policies, procedures and guidance) for effective data security and protection at the Company.
- Ensure staff and contractors are aware of their rights, duties and responsibilities on data security and protection, and the need to protect confidentiality.
- Ensure the Company's approach to information handling is communicated to all staff and made available to the public.
- Establish a working group (IG team) to undertake IG work activities, reporting and improvements.
- Ensure that appropriate data security and protection training is made available to all staff and completed as necessary to support their duties.
- Ensure annual assessments IG using the NHS Data Security and Protection Toolkit (DSPT) is completed to an acceptable level, submitted and published by 31 March of each year.
- Ensure audits of DSPT related policies and arrangements are carried out, documented and reported.
- Ensure IG improvement plan is in place, signed off by senior management annually and implemented.
- Oversee monitoring of information handling activities to ensure compliance with law and guidance.
- Oversee investigations into complaints about breaches of confidentiality or data protection, or freedom of information requests and oversee reporting/remedial action as required.
- Oversee the management and reporting of information incidents; and oversee corrective and preventive actions where required.
- Provide a focal point for the resolution and/or discussion of IG issues.
- Liaise with IG personnel from other organisations, committees, working groups and programme boards in order to resolve IG issues or promote IG standards.

Data Protection Officer (DPO)

The EU General Data Protection Regulation (GDPR) came into effect in UK Law from 25 May 2018. While the GDPR will not be directly applicable post-Brexit, the Government has confirmed that it will still apply. GDPR is supplemented by the Data Protection Act 2018 (DPA) and they must be read alongside each other to understand much of the law regarding data protection in the UK.

Under the GDPR, we are required to appoint a DPO, as our core activities include large scale processing of special categories of data (which includes information relating to an individual's health). Our DPOs perform their tasks independent of Company instructions, cannot be dismissed or penalised for performing their tasks, and report directly to the highest level of management (OPC Directors). We ensure that any tasks or duties we assign our DPOs do not result in a conflict of interests with their role as a DPO.
Current DPOs – **Francis Appiagyei** and **Sofia Carnelli**.
The DPO's responsibilities include:

- Informing and advising the Company about complying with GDPR/DPA and other data protection laws
- Monitoring compliance with GDPR/DPA and data protection laws – including staff training and internal audits
- Advising on and monitoring data protection impact assessments (DPIAs)
- Considering the risk(s) associated with the processing of data with regard to the nature, scope, context and purposes of the processing.
- Cooperating with the Information Commissioner's Office (ICO)
- Being the first contact published point for the ICO and citizens in terms of data processing

Information Asset Owners (IAOs):

IAOs are appointed by the SIRO to help oversee the integrity, access and security of the Company's information assets. The responsibilities of IAOs include but not limited to:

- Maintaining an understanding of the relevant assets, how they are used, what information is associated with the assets, the nature and justification of information flows to and from the assets.
- Knowing who has access to the assets and why. Ensuring use of the assets is checked regularly and that use remains in line with policy. This includes conducting monitoring and auditing procedures.
- Approve access to relevant assets.
- Approving arrangements where it is necessary for information from the assets to be put onto portable or removable media e.g. laptops, USB drives, and ensure information is effectively protected.
- Working with ISM to protect the asset against known and emerging risks.
- Ensuring risks to assets are identified, escalated to ISM, and the SIRO if necessary, documented and addressed.
- Supporting IG management of the assets as a member of the OPC IG Team. This includes supporting with investigations and disciplinary procedures into misuse of the assets.
- Compiling information and reports about the assets, including an annual written assessment to the SIRO for the assets owned.
- Ensuring the assets are documented and maintained on the Company's asset register.

Information Security Manager (ISM)

ISM (formerly information security officer) is vital role jointly head by the IT Manager and Technical Manger. ISMs are responsible for technical management of information security at the Company. The responsibilities of ISM (**currently Oliver Taylor and Tim Rijkaard**) include but not limited to:

- Informing and advising and implementing the Company's security posture including the effectiveness of access and security controls

- Monitoring compliance and/or certification with a range of legislation and standards which may include Network and Information Systems (NIS) Regulations, the security elements of GDPR data protection laws, Cyber Essentials, ISO 27001 and the Data Security and Protection Toolkit (DSPT)
- Responding and coordinating the response to CareCert alerts and advisories https://digital.nhs.uk/services/data-security-centre
- Monitoring and managing potential and actual security risks and incidents. Working with the SIRO and IAOs to ensure security risks (known and emerging) to assets are identified, documented and addressed
- Cooperating with NHS Digital, the ICO and National Cyber Security Centre (NCSC)
- Acting as a central point of contact on information security for both staff and external organisations.
- Supporting the SIRO and IG Lead with information security management, policies and procedures and their implementation
- Supporting the SIRO and IG Lead in ensuring that staff are aware of their responsibilities and accountability for information security.
- Compiling information and reports about information security, including annual written assessments to the SIRO, IG Lead and Company management.

POLICY

IG FRAMEWORK

The Company has a framework for IG. The IG framework is based on data security and protection by design and default, which is aligned with general NHS standards including the NHS Data Security &Protection Toolkit (DSPT).

SUPPORTING POLICIES

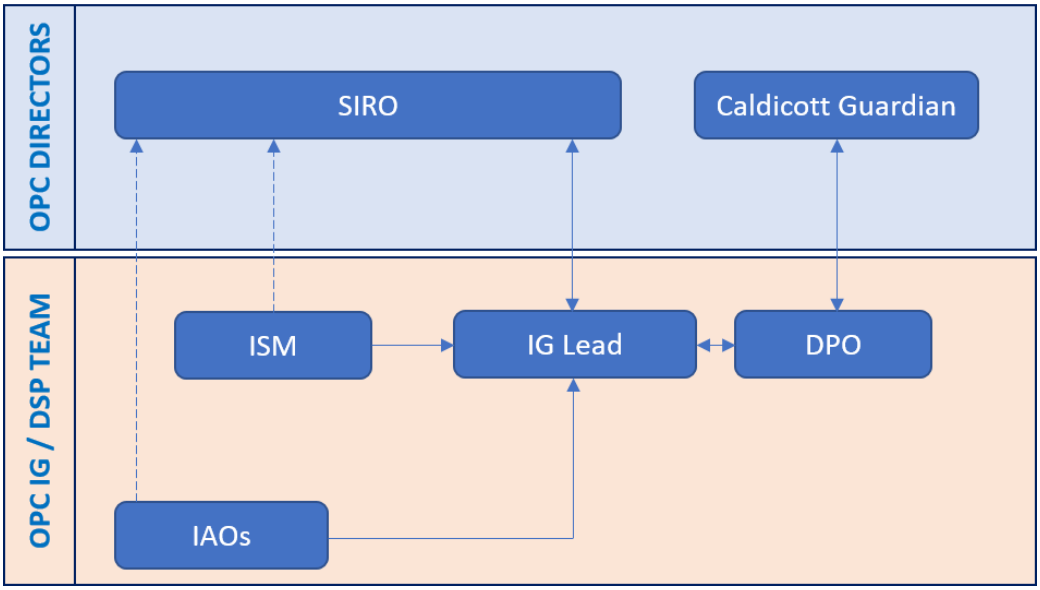
IG direction is set at board/management level, which is translated into effective organisational practices through the framework of IG or data security and protection policies, procedures, guidance, training, and transparency information. The key supporting policies include but not limited to:

- Data Protection
- Privacy Notice
- Confidentiality
- Information Security
- Acceptable IT Use
- Document and Records Management
- Data Quality
- Business Continuity

This policy list is not exhaustive and changes in the organisation may lead to additional documents or changes to this list.

ORGANISATIONAL STRUCTURE

The IG framework is based on data security and protection by design and default. For this to be effective, a clear organisational structure with roles, responsibilities and accountability is in place. The Company has an IG or data security and protection team (OPC IG/DSP Team), responsible for implementing and improving data security and protection at Company. IG improvement work (plan) is approved by senior management annually for continuous implementation.



IG PRINCIPLES

The Company recognises the need for an appropriate balance between transparency and maintaining confidentiality in the management and use of information of various types – personal information, confidential and commercially sensitive information, and non-personal (anonymised) information. The Company fully supports the principles of corporate, clinical and information 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, staff and information of a commercially sensitive nature. The Company also recognises the need to share information with other parties in a secure and controlled manner consistent with the interests of its service users and stakeholders.

The IG principles below underpin the Company's commitment to information governance

1. Openness
The Company shall:

- make non-confidential information available to the public through a variety of media as part of its openness ethos, including procedures and arrangements for handling queries from service users, the public, press and broadcasting media
- undertake annual assessments of its arrangements for openness via the DSPT
- maintain policies to ensure compliance with the Freedom of Information Act 2000 and the GDPR/DPA subject access rights pertaining to personal data

2. Legal Compliance
The Company shall:

- treat all identifiable personal information relating to patients as Confidential
- treat all identifiable personal information relating to staff, contractors and clients as Confidential except where legal or national security obligations requires otherwise
- establish policies and procedures to ensure compliance with the GDPR/DPA and data laws applicable to the UK
- undertake annual assessments of its compliance with legal requirements via DSPT
- establish and maintain policies, procedures and have agreements for the controlled and appropriate sharing of information with other parties

3. Information Security
The Company shall:

- maintain the National Data Guardian's Data Security Standards: https://www.gov.uk/government/publications/data-security-and-protection-for-healthand-care-organisations
- establish and maintain policies for the secure management of its information assets and resources
- undertake annual assessments of its information and IT security arrangements
- promote effective confidentiality and security practice to its staff through policies, procedures and training
- regularly maintained business continuity plans for all critical infrastructure components and core information systems
- establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential data breaches

4. Information Quality Assurance
The Company shall:

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

- undertake regular assessments 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
- ensure that wherever possible, information quality is assured at the point of collection

CALDICOTT PRINCIPLES

The Caldicott Principles or National Data Guardian recommendations (developed 1997; reviewed 2013) are a set of principles that organisations working within the NHS should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. The Company does not use patient identifiable information. However, when deciding whether to use information that would identify an individual, the Caldicott Principles should be used as a test.

https://www.gov.uk/government/publications/the-information-governance-review
https://www.dsptoolkit.nhs.uk/Help/23

The Caldicott Principles are:

Principle 1 - Justify the purpose(s) for using confidential information
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.

Principle 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).

Principle 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.

Principle 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.

Principle 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 are made fully aware of their responsibilities and obligations to respect patient confidentiality.

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

Principle 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.

DISSEMINATION & TRAINING

Dissemination: This document will be made available to staff and contractors via Smartsheet and NAS drive or on request from HR Department. This may also be in the form of a global notice sent to staff and contractors notifying them of the release of this document or made available on the Company website.

Training: Training on this document will be provided during induction of staff and contractors or as required by their training needs. Additional and/or regular training will be provided as necessary, based on training requirements to ensure continued awareness and compliance with this document.

MONITORING

Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Compliance with this document will be monitored by Company senior management or appropriate delegate. This may include regular and/or ad hoc compliance checks and audits where appropriate or warranted. This document is to be reviewed annually or sooner where necessary.

RELEVANT DOCUMENTS

Data Protection Policy
Privacy Notice
Confidentiality Policy
Information Security Policy
Acceptable IT Use Policy
Document and Records Management Policy
Data Quality Policy
Business Continuity Policy
Information Incident Reporting SOP
Audits and Monitoring SOP
Secure Transfer of Data SOP
Secure Destruction and Disposal of Data SOP
Staff Handbook

VERSION HISTORY

VERSION	EFFECTIVE DATE	REASON FOR CHANGE	AUTHORS
V1.0	06 MAR 2016	First final version of new policy	F. Appiagyei
V2.0	23 FEB 2017	Annual review and revisions	F. Appiagyei
V3.0	05 MAR 2018	Annual review and revisions	F. Appiagyei
V4.0	06 MAR 2019	Annual review and revisions	F. Appiagyei
V5.0	20 FEB 2020	New policy and new template	F. Appiagyei