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

Policy Number: POL 2300
Version Number: 5.0
Effective Date: 20 FEB 2020
Review Date: 20 FEB 2021

# INFORMATION SECURITY 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. 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 |
| IT | Information Technology |
| DSP | Data security and protection |
| DSPT | NHS Data Security and Protection Toolkit |
| GDPR | EU General Data Protection Regulation 2016 |
| DPA | Data Protection Act 2018 |
| DPO | Data Protection Officer |
| SIRO | Senior Information Risk Owner |
| ISM | Information Security Manager |
| IAO | Information Asset Owner |
| | |

## 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.

Information processing as a fundamental part of Company's business and service provision. Information security is essential to the Company's compliance with data protection legislation, maintenance of confidentiality and protection of its information assets.

## PURPOSE

This policy sets out the requirements placed on all employees and contractors (where applicable) for protecting the Company's information assets. The objectives of this policy are:

- to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Company;
- to describe the principles of security and explaining how they are implemented in the Company;
- to introduce a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities;
- to ensure that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies;
- to create and to maintain within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business;
- to protect information assets under the control of the Company.

The policy covers security which can be applied through technology and also people behaviour of those with access to information assets.

## 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.

## RESPONSIBILITY

**All Employees:**

- All employees must adhere to this policy. Information security is an obligation for all staff, as per data protection and confidentiality clauses in staff employment contracts.
- Any breach of data protection or confidentiality is a disciplinary offence, which could result in disciplinary action, termination of employment or legal action.
- All employees must report any information security incidents or concerns to the IT Manager or ISM.
- All employees must undertake the recommended annual data security and protection training and understand:
    a. What information they are using, how it should be protectively handled, stored and transferred.
    b. What procedures, standards and protocols exist for the sharing of information with others.
    c. How to report a suspected beach of information security within the organisation.
    d. Their responsibility for raising any information security concerns with the Head of Corporate ICT Technology & and Security

**Line Managers:**

- Ensure this policy is adhered to in their team and that there is on-going compliance.
- Ensure any information incidents and data protection breaches are reported, investigated and acted upon via the appropriate reporting procedure.

**HR Department:**

- Ensure this policy is included in inductions for all employees and contractors (where appropriate).
- Ensure appropriate action is taken to address non-compliance through staff disciplinary procedures.

**IT Manager/Information Security Manager (ISM):**

- Work with the SIRO and IG Lead to develop information security policies, procedures and guidance.
- Implement and enforce suitable and relevant information security procedures to ensure the Company's information systems and infrastructure remain compliant with the GDPR/DPA.
- Ensure that all information systems, network and equipment have adequate security measures to comply with GDPR/DPA and the DSPT.
- Provide adequate training to staff and users of the Company's information systems.
- Monito staff compliance with this policy and support on non-compliance investigations and disciplinary procedures.
- Manage the IT department to achieve the above responsibilities.

**Information Asset Owners (IAOs):**

- Approve access to relevant assets.
- Ensure third parties who access or use the asset have appropriate information security assurance
- Ensure use of the asset is checked regularly and that use remains in line with policy. This includes conducting monitoring and auditing procedures.
- Working with ISM to protect the asset against known and emerging risks.
- Ensuring risks to assets are identified, escalated to the ISM, and SIRO if necessary, documented and addressed.

**Senior Information Risk Owner (SIRO):**

- The SIRO has overall responsibility for information risk within the Company.
- Inform and advise the Company Directors on the effectiveness of information risk management across the Company.
- Approve the policy and ensure appointments are in place for information security at the Company.

**Senior Management:**

- Ensure that the policy and its supporting standards and guidelines are built into Company processes and that there is on-going compliance.
- Ensure all employees and contractors are aware of their responsibilities for information security.
- Ensure staff have appropriate training for the systems they are using and know how to access advice on information security matters.
- Determine the level of access to be granted to staff and contractors.

**Data Protection Officer (DPO)**

- Provide advice to the Company and all of its employees on data protection issues which can include confidentiality issues, in collaboration with the Caldicott Guardian.
- Monitor the Company's compliance with data protection laws (GDPR/DPA), including confidentiality.
- Report to the SIRO and directly to the Board in relation to data protection matters.

**Information Governance (IG) Lead:**

- Maintain the policy and ensure that processing and use of personal or confidential information contained within information assets are in line with data protection legislation and standards.
- Ensure employees and contractors are aware of the policy, procedures and user obligations applicable to their area of work.
- Ensure staff know how to access advice on information security matters.
- Ensure that appropriate information security and data protection training is made available to all staff and completed as necessary to support their duties.

## POLICY

### POLICY PRINCIPLES AND FRAMEWORK

The key principles which underpin this policy are to preserve:

- **Confidentiality** – access to information shall be confined to those with appropriate authorisation and protected from unlawful disclosure
- **Integrity** – information shall be complete and accurate; all information systems, assets and networks shall operate correctly in accordance with specification and intended purpose.
- **Availability** – information shall be available and provided to the right person when it is needed.

### INFORMATION SECURITY REQUIREMENTS – EMPLOYMENT CONTRACT

- Staff employment contracts shall contain information security requirement in the form of data protection and confidentiality clauses.
- Information security requirements of employees and contractors shall be included in job descriptions or clearly discussed and outlined during induction.

### SECURITY AND ACCESS CONTROLS

- The Company shall identify all information assets and classify those assets which contain personal data using guidance form the DSPT.
- All Company information assets, (hardware/equipment, software, application or data) shall have a named IAO, who shall be responsible for the information security of that asset.
- Access to information shall be restricted to users who have an authorised need to access the information and as approved by the relevant IAO or by the SIRO or delegate.
- Access to Company information assets (hardware, software, application or data) and computing facilities shall be controlled and restricted to authorised users.
- Approval to use Company information assets, in particular software or applications shall depend on the availability of a license from the supplier.
- To minimise loss of or damage to all assets, the IT department shall ensure that all IT and electronic equipment and assets shall be identified, registered and physically protected from threats and environmental hazards.

### COMPUTER AND IT NETWORK PROCEDURES

- Management of Company computers and IT networks shall be controlled through standard documented procedures including the Company's Acceptable IT Use Policy.
- This will also require agreed systems and processes with third party vendors working for and on behalf of the Company.

### INFORMATION RISK ASSESSMENTS

- All information assets will be identified and assigned an Information Asset Owner (IAO).
- IAOs shall ensure that information risk assessments are performed at least annually, following guidance from the SIRO or IG Lead.
- IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO and IG Lead for review.

**INFORMATION SECURITY INCIDENTS**

- All information security incidents, suspected or near misses must be reported to the IT Manager or ISM.
- All data protection or confidentiality breaches must be reported to the DPO or IG Team via the Company's Information Incident Reporting SOP.

**PROTECTION FROM MALICIOUS SOFTWARE**

- The Company and the IT department shall use software countermeasures and management procedures to protect itself against the threat of malicious software.
- All staff and users of the Company's IT shall be expected to cooperate fully with this policy and the Company's Acceptable IT Use Policy.
- Users shall not install software on the Company's IT without permission from the IT department. Users breaching this requirement may be subject to disciplinary action.

**REMOVABLE MEDIA**

- Where appropriate removable media should be encrypted. Removable media containing personal data must be encrypted. Please contact the IT department on encryption of removable media.
- Removable media that contain software require the approval of the IT department before they may be used on Company systems. Users breaching this requirement may be subject to disciplinary action.

**MONITORING SYSTEM ACCESS AND USE**

- An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis.
- The Company shall regularly audit and monitor compliance with this and other DSP policies.
- The Company reserves the right to monitor activity where it suspects that there has been a breach of this policy or other DSP policies. **The Regulation of Investigatory Powers Act 2000** permits monitoring and recording of employees' electronic communications including telephone communications for the following reasons:
    - Establishing the existence of facts investigating or detecting unauthorised use of the system
    - Preventing or detecting crime
    - Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
    - In the interests of national security
    - Ascertaining compliance with regulatory or self-regulatory practices or procedures
    - Ensuring the effective operation of the system.
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

**ASSURANCE OR ACCREDITATION OF INFORMATION SYSTEMS**

- The Company shall ensure that all new information systems, applications and networks have a system level security policy, accreditation or security assurance that can assure information security to standards that comply with GDPR/DPA.
- The system must be approved by the IT Manager, ISM or SIRO before it used for Company operations.
- Copy of assurance or accreditation should be held by the IT department for auditing purposes.

**SYSTEM CHANGE CONTROL**

- Changes to information systems, applications or networks shall be reviewed by the IT Manager and OPC IG Team with data protection impact assessment conducted.
- Changes to information systems, applications or networks shall be approved by the SIRO or Senior Management.

**BUSINESS CONTINUITY PLANS**

- The Company shall implement a business continuity plans which shall be compliant with DSPT guidance, reviewed and tested at least annually. Please refer to the Company's Business Continuity Policy.
- Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.
- The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested at least annually by the IT department.
- Staff must familiarise themselves with the Company's business continuity procedures. Please refer to the Company's Business Continuity Policy and Staff Handbook for further guidance.

**INFORMATION SECURITY TRAINING AND AWARENESS**

- Data Security and Protection training is mandatory and all employees and contractors (where applicable) are required to complete annual on-line Data Security Awareness training.
- All employees must read the Company Staff Handbook and policies and accept the declaration.

## 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

Acceptable IT Use Policy
Information Governance Policy
Data Protection Policy
Privacy Notice
Confidentiality Policy
Document and Records Management Policy
Data Quality Policy
Business Continuity Policy
Information Incident Reporting SOP
Audits and Monitoring SOP
Staff Handbook

## VERSION HISTORY

| VERSION | EFFECTIVE DATE | REASON FOR CHANGE | AUTHORS |
|---|---|---|---|
| V1.0 | 20 NOV 2014 | First final version of policy | HR department |
| V2.0 | 21 MAR 2016 | New policy and template | F. Appiagyei |
| V3.0 | 09 MAR 2018 | Minor revisions | F. Appiagyei |
| V4.0 | 09 MAR 2019 | Annual review and revisions | F. Appiagyei |
| V5.0 | 20 FEB 2020 | New policy and new template | F. Appiagyei |