DATA PROTECTION 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 / Data Protection Officer

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	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
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 personal information.

To provide quality services, OPC needs to collect and process personal and/or confidential information from staff, service users, suppliers, businesses and collaborators. The lawful and proper handling of personal information by OPC is important to the success of our business and in order to maintain the confidence of our service users, employees and collaborators. No matter how it is collected, recorded and used/shared, personal information must be handled in compliance with data protection laws applicable to the UK including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (EU) 2016/679 (GDPR).

PURPOSE

This policy sets out the Company's commitment to ensuring that any personal data, including special category personal data, which OPC processes, is carried out in compliance with data protection law. OPC ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

This policy sets out the requirements placed on all employees and contractors (where applicable) for protecting personal information or personal data defined as any information relating to an identified or identifiable natural person (living individuals), including patients, service users, employees and contractors. This document in conjunction with the Company's official **Privacy Notice** (https://optimumpatientcare.org/privacy-notice/), forms the entirety of the Data Protection Policy. Other relevant policies that support data protection include:

- Information Governance Policy
- Confidentiality Policy
- Information Security Policy
- Acceptable IT Use Policy
- Document and Records Management Policy
- Data Quality Policy
- Business Continuity Policy

APPLICABILITY

This policy applies to all personal data processed by OPC and is part of the Company's approach to compliance with data protection law. 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. Data protection is an obligation for all staff, as per data protection clause in their employment contract.
- Any breach of data protection is a disciplinary offence, which could result in disciplinary action, termination of employment or legal action.
- All employees must report any data protection breaches to an appropriate line manager.
- All employees must undertake the recommended annual data security and protection training.

- On receipt of a request by or on behalf of an individual for information held about them, or any other data subject's rights in relation to their personal data, staff will immediately notify the OPC IG Team by emailing dataprotection@optimumpatientcare.org.

Line Managers:

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

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 there are procedures in place for reporting confidentiality breaches.

HR Department:

- Ensure contracts for employees and contractors have data protection and confidentiality requirements.
- Ensure data protection is included in inductions for all employees and contractors (where appropriate).
- Ensure appropriate action is taken to address non-compliance through staff disciplinary procedures.

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. The GDPR is complemented by the Data Protection Act 2018 (DPA). Under the GDPR, OPC is required to appoint a DPO, as its core activities include large scale processing of special categories of data (which includes information relating to an individual's health). The Company's Information Governance Policy established this role.

The DPO's responsibilities include:

- Providing advice to the Company and all of its employees on data protection issues.
- Monitoring the Company's compliance with data protection laws (GDPR/DPA).
- Being the first point of contact in the Company's data protection matters.
- Reporting to the SIRO and directly to the OPC Directors in relation to data protection matters.

Caldicott Guardian:

- Ensure that data protection and confidentiality issues are appropriately reflected at Company board level and in Company strategies, policies and working procedures for staff.
- Provide advice on options for lawful and ethical processing and sharing of information in relation to disclosures of personal or confidential information.

Information Governance (IG) Lead:

- Oversee development, implementation, monitoring and awareness of the Data Protection Policy.
- Ensure the Company's approach to data protection is communicated to all staff and the public.
- Ensure that appropriate data security and protection training is made available to all staff and completed as necessary to support their duties.
- Oversee the management and reporting of information incidents; and oversee corrective and preventive actions where required.

POLICY

INFORMATION COVERED BY DATA PROTECTION LEGISLATION AND THIS POLICY

Data protection ensures that we only collect, process, use of share personal data lawfully. It ensures that a person's right over their own personal information is respected. The data protection laws for the UK are the General Data Protection Regulation (EU) 2016/679 (**GDPR**) and the Data Protection Act 2018 (**DPA**). The DPA is the UK's implementation of the GDPR. Please visit the links below to learn more about the GDPR and DPA.

- https://www.gov.uk/data-protection
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Personal Data: Any information relating to an identified or identifiable natural person i.e. living individuals (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The GDPR applies to personal data.

Pseudonymised Personal Data: Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. This the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The GDPR applies to pseudonymised personal data. Pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR.

Anonymised Data: This is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GDPR and DPA do not apply to anonymised or aggregated data (provided the anonymisation or aggregation is not done in a reversible way), as it is not personal data.

DATA PROTECTION PRINCIPLES

The following principles must be adhered to by all OPC employees and contractors:

The 7 key principles of the GDPR/DPA, which OPC abides by, requires that **Personal Data shall be**:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals [*Lawfulness, fairness and transparency*].
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes [*Purpose limitation*].
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed [*Data minimization*].
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay [*Accuracy*].

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals [*Storage limitation*].
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures [*Integrity and confidentiality (security)*].
7. The data controller shall be responsible for, and be able to demonstrate compliance with, the GDPR principles [*Accountability*].

The Company will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

The Company's policy on how we handle personal data is covered in the official **PRIVACY NOTICE** of the Company, which is updated regularly. You must read the Company's Privacy Notice in conjunction with this document as part of the full Data Protection Policy: **https://optimumpatientcare.org/privacy-notice/**

If staff have any concerns about data protection, they must raise in the first place with the OPC IG Team by emailing **dataprotection@optimumpatientcare.org**. The OPC IG Team will then consult the DPO if necessary, before advising.

ADDITIONAL GUIDANCE:

Disclosing Personal Information

To ensure information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the ICO's Anonymisation Code of Practice (https://ico.org.uk/).
- When there is consent from the data controller or owner.
- When the information is required by law or under a court order or to prevent fraud or serious crime. In this situation staff must discuss with the IG Lead; the IG Lead will then consult the DPO or Caldicott Guardian if necessary, before advising on disclosure.

Information that is properly de-identified or anonymised is not Personal Data and can be disclosed without breaching data protection. OPC operates a de-identified service. Personal information, wherever appropriate, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice:
https://ico.org.uk/media/1061/anonymisation-code.pdf

Transferring Personal Data

Care must be taken in transferring personal or confidential information to ensure that the method used is secure.

- Transferring personal or confidential information by email should be encrypted wherever possible.
- Sending personal or confidential information via unencrypted email is only permissible where the risks of using unencrypted email have been explained to the recipient and the recipient has accepted the risks and given their consent.
- All staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and postal mail.

Please note that the Company is not responsible for the privacy and data protection practices of other organisations or websites which may be reached through links contained in our websites, social medial or information platforms.

DATA SUBJECTS RIGHTS:

The Company has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.
All requests will be considered without undue delay.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data has been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if OPC was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless OPC can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

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

Information Governance Policy
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
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	02 MAR 2017	Annual review and revisions	F. Appiagyei
V3.0	02 JUL 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