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

Policy Number: POL 2200
Version Number: 5.0
Effective Date: 20 FEB 2020
Review Date: 20 FEB 2021

CONFIDENTIALITY 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	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.

It is important that OPC protect and safeguard person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law [Data Protection Act 2018 (DPA) and the General Data Protection Regulation (EU) 2016/679 (GDPR)] and to provide assurance to staff, service users, suppliers, businesses and collaborators.

PURPOSE

This policy sets out the requirements placed on all staff when sharing information. It lays down the principles that must be observed by employees and contractors (where applicable) who have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their employment contractual responsibilities but also a requirement within the **common law duty of confidence** and data protection legislation i.e. GDPR/DPA.

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. Confidentiality is an obligation for all staff, as per Confidentiality clause in their employment contract.
- Any breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in disciplinary action, termination of employment or legal action.
- All employees must report any confidentiality breaches to an appropriate line manager.
- All employees must undertake the recommended annual data security and protection training.

Line Managers:

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

HR Department:

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

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.

Data Protection Officer (DPO)

- To 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.
- Monitoring the Company's compliance with data protection laws (GDPR/DPA), including confidentiality.

Caldicott Guardian:

- Responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to the Company and staff.
- Ensures that data protection and confidentiality issues are appropriately reflected at Company board level and in Company strategies, policies and working procedures for staff.

Senior Information Risk Owner (SIRO):

- Approve and take accountability for risk-based decisions and reviews with regards to the use, disclosure or processing of confidential data in regard to the operating functions of the Company.

Information Governance (IG) Lead:

- Ensure the policy is kept up to date, providing advice on request to staff on confidentiality issues.
- Ensure that training is provided for all staff groups to further their understanding of the principles of confidentiality and their application.
- Ensure the Company's approach to confidentiality is communicated to all staff and the public.
- Oversee the management and reporting of information incidents; and oversee corrective and preventive actions where required.

POLICY

CONFIDENTIAL INFORMATION

The following types of information are regarded as confidential information and are subject to this policy.

Person-identifiable information or Personal data: Any information that contains the means to identify a person, e.g. name, address, postcode, date of birth, etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information: This is defined here as personal data which is not person-identifiable data but should however be treated with a high level of confidentiality as they may carry a potential risk of perpetuating any stigma that may be associated with them e.g. sexually transmitted diseases, termination of pregnancy, fertility treatments, marital status, complaints, convictions or imprisonments, abuse (physical, psychological or sexual by others), etc.

Information provided in confidence: This is any information that is disclosed in confidence and the data provider/controller expect that information to be treated confidentially. It can include names and addresses as well as a person's sensitive personal information, family members, etc. It also includes confidential Company information and management discussions (staff, contractors and service users).

Non-person identifiable information: This can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

CONFIDENTIALITY PRINCIPLES

OPC responsible for protecting all the information it holds and must always be able to justify any decision to share information. All employees and contractors must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your Line Manager or the IG Lead.
- Person-identifiable information, wherever appropriate, in line with the data protection principles stated in the Data Protection Policy, 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.
- Access to rooms and offices where computers are present, or person-identifiable or confidential information is stored must be controlled, to prevent access to information by unauthorised persons.
- All staff should maintain a clear desk policy; and must keep all records containing person-identifiable or confidential information in storage places that are locked.
- Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

- OPC employment contract includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.
- If staff have any concerns about confidentiality or disclosing information, 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 or Caldicott Guardian if necessary, before advising.

A summary of **Confidentiality Do's and Don'ts** can be found at **Appendix A**.

A summary of the **Legal Framework** for confidentiality which forms the key guiding principles of this policy can be found in **Appendix B**.

Please refer to the Company's Information **Incident Reporting SOP** on how to report a breach of this policy.

DISCLOSING PERSONAL/CONFIDENTIAL 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 de-identified or 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. Person-identifiable 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.

WORKING AWAY FROM THE OFFICE ENVIRONMENT

`

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry Company or work-related information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

- Taking home or removing paper documents that contain personal or confidential information from the Company premises and/or participating GP practices is discouraged.
- To ensure safety of confidential information, staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them to another location.
- If staff do need to carry personal or confidential information, they must ensure that it is in a sealed non-transparent container i.e. windowless envelope, suitable bag. Confidential information is kept out of sight whilst being transported. Any electronic removable media must be encrypted.
- If staff do need to take personal or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends must not be able to see the content or have any access to the information.
- Staff must not forward any personal or confidential information via email to their private email account or store personal or confidential information on a privately-owned computer or device.

CARELESSNESS

All staff have a legal duty of confidence to keep personal or confidential information private and not to disclose information accidentally. Individual staff may be held personally liable for a breach of confidentiality and must not:

- talk about personal or confidential information in public places or where they can be overheard;
- leave any personal or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents; and
- leave a computer or IT devices logged on to a system where personal or confidential information can be accessed, unattended.

Staff in management roles must not disclose information discussed with them in confidence by senior management with other staff.

Steps must be taken to ensure physical safety and security of personal or confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct and may lead to disciplinary and/or legal action.

ABUSE OF PRIVILEGE

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the GDPR/DPA. This is particularly important for staff who work with GP practices.

CONFIDENTIALITY AUDITS

Good practice requires that all organisations that handle personal or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems and procedures to evaluate the effectiveness of controls within these systems.

Confidentiality compliance monitoring and auditing is coordinated by OPC IG Team, which includes an annual audit and regular or ad hoc spot-checks as part of the DSPT assessments.

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
Data Protection Policy
Privacy Notice
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	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

APPENDIX A

CONFIDENTIALITY DOs AND DON'Ts

DOs

- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Only transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

DON'Ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't allow any person-identifiable information to leave a GP practice.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

APPENDIX B

SUMMARY OF LEGAL FRAMEWORKS

GDPR AND DPA

OPC is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and contractors of OPC, who may be held personally accountable for any breaches of information security for which they may be held responsible.

OPC shall comply with the following legislation and guidance as appropriate:

The General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA), which regulate the use of "personal data" and sets out principles to ensure that personal data is:

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*].

COMMON LAW DUTY OF CONFIDENTIALITY

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

HUMAN RIGHTS ACT (1998)

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

CALDICOTT PRINCIPLES

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect confidentiality.

COMPUTER MISUSE ACT (1990)

The Computer Misuse Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access to data or programs held on a computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts with intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.