DATA QUALITY POLICY

V2.0 21 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:	21 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
IAO	Information Asset Owner
ISM	Information Security Manager
ICO	Information Commissioner’s Office
CHI	Community Health Index (Scotland)
HCN	Health and Care Number (Northern Ireland)
PID	Person identifiable data or patient identifiable data

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.

Data quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever this is required. Reliable and acceptable data quality is fundamental in supporting the operations and services of the Company. Decisions made at the Company, whether operational, managerial or financial need to be based on information which is of the highest quality.

PURPOSE

This policy sets out the policy framework and requirements placed on employees and contractors (where applicable) for maintaining data quality at the Company. The availability of complete, accurate, relevant, accessible and timely data is important in supporting delivery of reporting services to service users. It is vital in for management and planning, contracting and accountability. A data quality policy and monitoring of data standards is a requirement of the DSPT.

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 are responsible for implementing and maintaining data quality.
- All employees must maintain accurate information legally (as per the GDPR/DPA), contractually (as per contract of employment) and ethically (as per professional codes of practice).

Line Managers:

- Ensure this policy is adhered to in their team and that there is on-going compliance.
- Ensure that data is accurate and as complete as possible for their area of work.

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 to rectify data quality issues and to improve data quality.

Data Protection Officer (DPO)

- To provide advice to the Company and all of its employees on data protection issues which can include data quality (accuracy of information).
- Monitoring the Company's compliance with data protection laws (GDPR/DPA).

Senior Information Risk Owner (SIRO):

- Approve and take accountability for risk-based decisions and reviews with regards to the quality of data (information assets) of the Company.
- Ensure IAOs are identified and appointed to manage all information assets including maintaining quality of the data held in the assets.

Information Asset Owners (IAOs):

- IAOs of critical information assets such as databases have an important responsibility to ensure that data collected, processed and stored is of high quality in line with industry standards and this policy.
- Know what information is held in the asset, the nature and justification of information flows to and from the asset they are responsible for.
- Provide data quality training to individuals who use or access the asset.
- Ensure use of the asset is checked regularly and that use remains in line with policy. This includes conducting monitoring and auditing procedures.
- Ensuring risks to assets and quality of data are identified, escalated to the ISM, and SIRO if necessary, documented and addressed.
- Ensure the asset is documented and maintained on the Company's information asset register.

Information Security Manager (ISM)

- Work with the SIRO and IG Lead to develop information security policies, procedures and guidance to maintain and improve data quality.
- Ensure that all information assets have adequate security measures to comply with GDPR/DPA and the DSPT. This includes working with IAOs to ensure data quality is maintained and improved.

Information Governance (IG) Lead:

- Ensure the policy is kept up to date, providing advice on request to staff on data quality with respect to collection, storage, processing and reporting of personal information.
- Ensure that training is provided for all staff groups to further their understanding of the principles of data quality.
- Work with IAOs in the management and reporting of information incidents relating to data quality; and oversee corrective and preventive actions where required.

POLICY

GENERAL PRINCIPLES

- All data collection, manipulation and reporting processes by the Company will be covered by clear procedures where appropriate, which are easily available to all relevant staff, and regularly reviewed and updated.
- Data processes at the Company must comply with this policy including data protection laws. This will include audits and monitoring checks on sample data.
- Staff must conform to legal (GDPR/DPA), regulatory (e.g. research ethics committee), and data quality standards set in this policy, to ensure data quality is maintained and improved.
- All staff should be aware of the importance of good data quality and their own contribution to achieving it and should receive appropriate training in relation to data quality aspects of their work.
- Teams should have comprehensive procedures in place for identifying and correcting data errors, such that information is accurate and reliable at time of use.

DATA QUALITY STANDARDS

Data is of good quality if it is fit for intended uses in operations, service delivery, decision making and planning. All employees and contractors (where applicable) must ensure that the following data quality standards are adhered to:

Validity

- All data items held on Company systems must be valid.
- Where codes are used, these will comply with national standards or map to national values or comply with standards set by the OPC Data Team.
- Company systems will include validation processes, ideally at data entry, input or upload stage, to check in full or in part the acceptability of the data wherever possible. This facility should not be disabled or overridden by staff without prior approval from the IAO.
- Where possible validation processes should use accredited external sources of information e.g. using National Administrative Codes Set (NACS) to check organisation/GP practice codes.

Accuracy

- Data recorded manually and on computer systems must be accurate. All recorded data must be correct the first time it is entered.
- At data entry or input, data accuracy is the direct responsibility of the person entering the data supported by their line manager.
- Recorded data may be updated, where appropriate, to correct the accuracy of the information.
- The accurate recording of data items is must for all staff, as inaccurate data may lead to data protection breaches, incorrect/bad decisions and other adverse outcomes for the Company and its services.

Completeness

- All mandatory data items within a dataset must be completed, where possible and practical.
- Use of default codes will only be used where appropriate, and not as a substitute for real data.
- If it is necessary to bypass a data item in order to progress the delivery of services to a service user or client, the missing data must be marked or reported for follow-up by the IAO of the relevant system.
- Guidance on handling missing data in the Company's Document and Records Management Policy should be followed.

Consistency

- Data collection or recording must be consistent for a given information system.
- Required standards should be set by the relevant IAO for staff who use that asset or system to follow.
- Duplicate data items between different systems must be consistent so as not to lead to any ambiguity between different data sources.

Coverage

- Data collected or received should meet the required scope and specification for that data – i.e. data capture must be complete wherever possible.
- Data quality checks must be undertaken to assure that data coverage is complete before the data is accepted into the information system e.g. data extracted from GP practice should be checked for completeness before it is uploaded into the required database.
- Where possible accredited external sources of information should be used to check for good coverage e.g. using NHS prescribing data for therapy data received, using QOF data to check for data relating to know and regularly reported indicators, etc.

Timelines

- Data should be entered or recorded in timely manner for service delivery and business operation.
- Data should be recorded or submitted to agreed deadlines. For general staff this includes recording or submitting data to timelines set by management. For management this includes recording or submitting data to timelines set by senior management or as required by the service user or client.
- In the event of delays, reasons and mitigation plan must be provided.

PERSON IDENTIFIABLE DATA (PID)

- Person identifiable data or patient identifiable data (PID) (also known as personal data), may only be processed and used when consent is provided by the person (data Subject) or data controller; or where the processing and use of the PID without consent is covered by legislation – the GDPR/DPA, or Section 251 approval from HRA CAG.
- Please refer to the Company's Data Protection Policy and Confidentiality Policy for guidance on use and disclosure of PID.
- All data received from Company service users including GP practices for secondary uses i.e. for non-direct healthcare, must always be pseudonymised or anonymised. Secondary Uses means any use of data outside of direct patient care. This includes processing data or information for research purposes, audits, service management, commissioning, contract monitoring and reporting.
- PID and sensitive data such as sexually transmitted diseases, termination of pregnancy, fertility treatment, marital status, convictions/imprisonments, physical/psychological/sexual abuse must be removed from data at source (at the GP practice) prior to pseudonymisation.

PSEUDONYMISED DATA

Pseudonymisation means 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.

Person identifiable data which have undergone pseudonymisation (Pseudonymised Data) are used when they are shared with persons for secondary uses. A unique identifier is used and only those with the 'key' i.e. the GP practice can re-identify persons from the data.

- The Company applies robust pseudonymisation techniques to all data received from GP practices at source (at the GP practice). These techniques encompass the replacement of NHS number, CHI number or HCN of patient at a GP practice with an alternative unique identifier.
- Pseudonymisation must always require a SALT (i.e. an extra string of characters appended to the data that is being pseudonymised), which must never be held on Company information systems. SALT key may be held by the data controller i.e. GP practice or by a trusted third party.
- Data which includes the date of birth and the postcode is not suitable for pseudonymisation.
- Date of birth must always be replaced with year of birth i.e. age.
- Full post code must be replaced with district level code only i.e. the first part of the postcode only.
- Pseudonymised data are still considered personal data or PID and must be treated securely and appropriately.
- A data sharing agreement or service agreement must always be in place before pseudonymised data are to be transferred from a service user i.e. GP practice to OPC or to a third party.
- It is criminal offence and breach of data protection laws for any person to attempt to re-identify persons from data that has been pseudonymised or anonymised. Any staff or contractor who attempts to re-identify a person from such data will face severe disciplinary action include immediate dismissal and legal action.
- Please refer to the Company's Data Protection Policy and Confidentiality Policy for guidance on use and disclosure of PID or personal data.

ANONYMISED DATA

Anonymisation is the process of turning data into a form that does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

- All data provided to third parties from the Company's research databases must always be anonymised.
- Wherever possible data provided to from the Company's research databases must be aggregated.
- Anonymised data must not be provided to third parties from the Company's research databases without governance or ethics approval and a data sharing agreement.
- It is criminal offence and a breach of data protection laws for any person to attempt to re-identify persons from anonymised data. Any staff or contractor who attempts to re-identify a person from such data will face severe disciplinary action include immediate dismissal and legal action.

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
Confidentiality Policy
Information Security Policy
Acceptable IT Use Policy
Document and Records Management 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	31 AUG 2017	First final version of new policy	F. Appiagyei
V2.0	21 FEB 2020	New policy and new template	F. Appiagyei