SECURE TRANSFER OF DATA SOP

V3.0 10 MAR 2020

This is a Controlled Document. This standard operating procedure (SOP) is issued by the Company. Failure to comply with this SOP may lead to disciplinary and/or legal action where appropriate. Human Resources Department and/or appropriate delegate should ensure the SOP 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 Director

Signature: 

Date: 10 March 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
IT	Information Technology
IG	Information Governance
DSP	Data security and protection
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

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 or data transfer is a fundamental part of service provision and business operations. Data must be transferred securely to ensure compliance with data protection laws and confidentiality where applicable.

The Company operates a de-identified data service which means that transfer of patient identifiable data without consent or appropriate legal basis is strictly prohibited. This document forms part of the Company's Information Security policy and the wider Information Governance policy.

PURPOSE

This SOP provides guidance to employees and contractors (where applicable) on secure transfer of data.

APPLICABILITY

This SOP applies to Company staff, and associated persons such as secondees, third party and freelance contractors. This SOP also an essential reading for all line managers regarding reporting and managing IG incidents. Compliance with this SOP is a legal and contractual duty for staff and contractors. Failure to comply with this SOP may lead to disciplinary and/or legal action.

RESPONSIBILITY

All Employees:

- All employees are responsible for complying with procedures for secure transfer of data and must adhere to this SOP.
- All employees must ensure that no Confidential or Personal Data is disclosed during secure transfer of data without appropriate consent.
- All employees must ensure that no patient identifiable data is transferred without consent to maintain the Company's de-identified data service provision policy.
- All employees must report any data breach from transfer of data.

Line Managers:

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

HR Department:

- Ensure appropriate action is taken to address non-compliance through staff disciplinary procedures.
- Ensure this SOP is disseminated to staff and is part of ongoing staff training.

Senior Management:

- Ensure appointments or delegated responsibilities are in place for facilitating and managing secure data transfers at the Company.

- Provide approval for secure transfer of records, business critical information and datasets at the Company.

Data Protection Officer (DPO)

- Monitoring the Company's compliance with data protection laws (GDPR/DPA) when data is destroyed or disposed of.

Senior Information Risk Owner (SIRO):

- Responsible for providing general guidance on information security and secure transfer of data.
- Oversee development of policies and procedures for secure destruction or disposal of data.

Information Governance (IG) Lead:

- Ensure information governance considerations including confidentiality, data protection and Caldicot Principles are maintained in data transfers.
- Ensure that training is provided for all staff groups to further their understanding of the principles of IG, data protection and confidentiality.

Information Security Manager (ISM) / IT Department

- Oversee procedures and measures to ensure secure access, use and transfer of data for all information system.
- Provide methods and facilities for secure transfer of data that meet industry or NHS requirements.
- Undertake and document regular monitoring and audits to ensure compliance with secure data transfer.

Information Asset Owners (IAOs)

- Ensure this SOP is adhered to and that there is on-going compliance for secure transfer of data contained in the asset they own.

PROCEDURES

BASIC GUIDANCE

- Never send or receive person or patient identifiable data without consent or appropriate legal basis. The Company operates a strict de-identified data service.
- Ensure there is information governance considerations prior to data transfer.
- Ensure there is appropriate data sharing agreement or authorisation is in place for the data transfer.
- Ensure data is encrypted where appropriate before transfer.
- Ensure correct details of the data recipient are in place for data transfer.
- Ensure data is transferred via a secure, suitable and approved route.
- Ensure confirmation of safe receipt of data by the data recipient is received.
- Report any issues or suspected breaches to the relevant line manager, IT department or OPC IG Team. Follow the Company's Incident Reporting SOP.

NHS INFRASTRUCTURE/N3/HSCN DATA TRANSFERS

- Due to the inbuilt information security functionality (e.g. NHSmail, Secure File Transfer Service), the NHS infrastructure provides a highly secure method of transfer of data.
- Where the use of nationally provided infrastructure services is not possible, information transfer standards and procedures must be agreed and established between the sender and recipient to ensure IG and data protection assurance is in place.
- All GP practices data extracts must be transferred via secure N3 or HSCN (Health and Social Care Network) or a secure route e.g. SFTP agreed with the GP practice.
- Data for data linkages must be transferred via secure N3 or HSCN or secure route agreed with the data sender or recipient.
- Data relating to GP practices and patient data must be encrypted during transfer.

OPC DATABASE TRANSFERS

- All data must be transferred securely into any OPC database including but not limited to OPCSD and OPCRD.
- All data transfers from OPCRD including datasets must be via secure route e.g. SFTP or secure VPN or a secure route agreed with the data sender or recipient.
- Ensure appropriate data sharing agreement or permission is in place for any OPC database transfer.
- Database transferred must always be encrypted during transmission/transit.

ENCRYPTED TRANSFER AND PASSWORD PROTECTION OF FILES

- Password protecting files is recommended to help prevent casual compromise if the file is sent to the wrong recipient.
- Electronic data must be encrypted for external data transferred outside. Industry or NHS encryption standards should be applied.
- Request encryption of data from the IT dept. (email: IT@optimumpatientcare.org) prior to the transfer of data.
- IT dept. will undertake appropriate encryption of the data to be transferred and should provide the relevant encryption key(s) which must be transferred separately to the data they relate to.
- Data sender must ensure they receive confirmation of safe receipt of the data from the data recipient and notify the IT dept.
- Some data may be transferred without encryption as deemed appropriate by IT dept. or SIRO based on risk assessment and IG considerations.

TRANSFERS OF DATA STORED ON REMOVABLE MEDIA

- Use of removable media for the purposes of storing personal or otherwise sensitive data must be subject to an information risk assessment by the Information Asset Owner (or equivalent). Please seek guidance from the IT Dept. or SIRO or IG Lead.
- Data should be encrypted wherever possible and appropriate

TRANSFERS OF UNENCRYPTED DATA BY COURIER OR POST

- Transfer of unencrypted data by post or courier is strictly prohibited.
- This is poor practice which goes against the ethos of the Company.

SECURE TRANSFER BY POST

The relevant line manager will need to define the service levels arrangements required from the private or Royal Mail postal service provider for your mail:

- Secure post – is a signature required or not required?
- Track and trace facility – is this available at individual bag or item level to ensure that items can be identified at any appropriate point in the mail pipeline?
- Redirected post – are there guaranteed arrangements for this?
- Undeliverable post – what are the arrangements for this?

SECURE TRANSFER BY COURIER

- A 'Secure' Courier is not an internal postal service or member of staff visiting a location who may act as a 'casual courier' (which some organisations refer to as "couriers").
- A 'Secure' Courier will provide a secure and tracked mode of collection and delivery rather than a 'by hand' / personal delivery service. Some 'Secure' Courier services allocate a container to an organisation's items while others may store them in the same container as other organisations' courier items at lesser cost.
- A 'Secure' Courier will be an organisation providing courier services which provide adequate security assurances set out in a written contract.
- The relevant line manager will need to determine the need and provider for transfers by courier.

VERBAL COMMUNICATIONS

- The security and confidentiality of telephone and personal conversations should be considered. It is a compulsory requirement for all staff to complete the basic IG training which covers this subject.
- Staff should be mindful of the need to maintain security and confidentiality when discussing personal or other sensitive information.

TELEPHONE ANSWERING MACHINES

- The Company operates an internet phone services provided securely by Voipfone – an accredited internet telephone service provider.
- Voicemails are delivered to the relevant staff work email account.
- Recorded telephone messages may contain personal or sensitive information such as names and addresses of service users, details of health or social care professionals phoning with queries about service users or applicants for jobs advertised.
- Voicemails received or recorded should not be forward outside work-related networks without prior approval from your Dept. Head or Line Manager
- Consideration should be given to which staff members have access to answering machines
- Physical protection should be considered hence all office phones should be located in a lockable office

EMAIL

- Email is essential for daily work and communications. Email is an easily accessible media for transferring data.
- Employees and contractors must never transfer patient identifiable data via email.

- Company email accounts must be used in accordance with the Information Security Policy and the Acceptable IT Use Policy.
- Ensure data is appropriately encrypted prior to data transfer via email.
- Seek guidance from IT Dept. for transfer of confidential data via email. Please write in your email subject 'CONFIDENTIAL INFORMATION' when sending email with confidential data.

GOOGLE APPLICATIONS

- The Company receives service from Google Application including but not limited to Gmail, Google Drive, Google Docs, Google Forms, Google Calendar, etc.
- Google applications are all operated via password protected user access.
- Data can be stored and shared access provided via Google applications
- No patient identifiable information should be shared via Google applications
- The relevant line manager should determine the suitability to share data via Google applications.
- IT Dept. will determine if Google applications should be arranged for the data recipient.
- IT Dept. will provide password log in accounts for external data recipient.
- Where access to data via Google applications is no longer required, please inform IT Dept. to remove access and delete accounts.

SMARTSHEET

- Smartsheet is operated via password protected user access.
- Data can be stored and shared access provided via Smartsheet.
- No patient identifiable information should be shared via Smartsheet.
- The relevant line manager should determine the suitability to share data via Smartsheet.
- IT Dept. will determine if separate Smartsheet workspace should be arranged for the data recipient.
- IT Dept. will provide password log in accounts for external data recipient.
- Where access to data via Smartsheet is no longer required, please inform IT Dept. to remove access and delete accounts.

ELECTRONIC MESSAGING APPLICATIONS (EMAs)

- EMAs include text and instant messaging applications and platforms
- The benefits of using EMAs to transmission personal information must be weighed against the risks of confidentiality and data breaches.
- The current Company guidance is that EMAs are not suitable for transmission of personal or confidential data, as the risks of breaches are unacceptable for secure data transfer

FAX AND eFAX

- Fax containing confidential or sensitive data should be subject to safe haven principles and procedures or the equivalent to ensure faxes are safely stored, sent and received and communicated to the recipient.
- eFax software allows users to send or receive a fax via a computer rather than a fax machine. eFax should also be subject to safe haven principles.
- The IG risks for eFax are a combination of the risks linked to email and standard fax communications. The Company deems this is suitable for data transfer subject to IG considerations from the relevant line management, SIRO or IG Lead.

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.

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 SOP 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
Data Quality Policy
Business Continuity Policy
Information Incident Reporting SOP
Secure Destruction or Disposal of Data SOP
Staff Handbook

VERSION HISTORY

VERSION	EFFECTIVE DATE	REASON FOR CHANGE	AUTHORS
V1.0	06 MAR 2015	First final version of new policy	F. Appiagyei
V2.0	09 MAR 2018	Review and minor revisions	F. Appiagyei
V3.0	10 MAR 2020	Review and major revisions and new template	F. Appiagyei