OPS37 Compliance in Records Management

Document Control

Policy Title	Compliance in Records Management
Number	OPS37
Effective Date	11/06/2021
Version	2.2
Review due	31/05/2025
Classification	Unrestricted
Owner	Governance & Quality Assurance
Author	
Reviewer	

Revision History

Version	Date	Description
1.0	02/03/2015	Original Document
1.0	31/07/2016	Original Effective Report Writing & Recording of Care Given Policy
2.0	15/04/2018	Major changes have been applied to this policy to combine two separate policies into a single comprehensive policy document.
2.1	31/05/2020	Review, revisions, and updates on links.
2.2	08/06/2021	Minor updates to reflect Brexit and UK GDPR

Document Approvals

Approver	**Name**	**Date**
Head of Finance, Compliance & Performance		11/06/2021
Chief Executive Officer		11/06/2021

This page is intentionally left blank.

Contents

1. Introduction

Managing Optalis records efficiently and effectively to support day to day operational and business activity supports the company in meeting certain legal requirements. As we create and collect increasing amounts of information about our customers, staff, and business activities, it is vital that as a company we can organise, securely store and retrieve this information when required. Under data protection legislation, staff and customers are entitled to access to their records and information and need to be assured that their personal data is being held both confidentially and securely.

This policy is structured to provide staff with guidance on managing records through their life cycle from creation to disposal. Adherence to this guidance will support all aspects of the company and support the compliance with its duties as a public body subject to the Public Records Act (1958) and the Freedom of information Act (2000); both of which can be found within the References section below.

2. Scope

This policy and its supporting guidelines and tools are for the use of all Optalis staff. The obligation of all staff is to recognise that the information they create or use daily has a value to Optalis as **information assets**. This carries with it a responsibility to manage those assets on behalf of Optalis in line with legal, business and shareholder obligations and to ensure that records are accessible, accurate, kept in good condition and either held permanently or disposed of in a timely fashion as appropriate.

This policy applies to all recorded information, regardless of format, that documents the output of, or relates to, Optalis' actions and transactions during its business activities. Records are evidence of business transactions or decisions which are fixed in time. They contain content (information), context and structure. The use or re-use of the information that changes any of these three factors results in the creation of a new record of a different transaction.

3. Purpose

Optalis' records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily operational functionality; supporting consistency, continuity, efficiency and productivity, and helping to deliver services with the level of quality and compliance that Optalis upholds. Adherence to the guidance provided in this Policy will provide Optalis with several benefits including:

- Better use of physical and server space
- Better use of staff time
- Improved control of valuable information resources
- Compliance with legislation and standards
- Reduced costs

This policy sets out a framework within which Optalis' records can be managed and

controlled effectively, in alignment and adherence with legal operational and information needs. This policy applies to all Optalis records held in any format including:

- Paper
- Photographs and other images
- Audio and video, USB, CD ROM, etc.
- Computerised records
- Scanned records
- Text messages and social media
- Websites and intranet sites that provide key information to customers

4. Policy Statement

The purpose of this policy is to:

- Define duties and responsibilities in regard to records management throughout Optalis
- Outline the key legal obligations and statutory provisions that apply to records created and used throughout Optalis
- Provide a procedural Framework with guidance to encourage best practice in records management
- Describe the 'Information Life Cycle' and highlight best practice to be followed at each stage of the cycle from creation to disposal

5. Policy Principles

All records are a legal account of our operations; staff **must** ensure professional language and an objective, respectful and factual approach must be used throughout any written document or communication (including email, messenger, Teams etc.). Staff must avoid subjective opinion where possible and ensure a timestamp and signature as an acknowledgement of the interaction. Any abbreviations should be explained when first used, e.g., Wokingham Borough Council (WBC).

To meet the requirements of the policy it is essential that all staff understand and practice the following principles when managing their recorded information regardless of its format:

- All information created during normal Optalis activity is the property of Optalis. Every employee has a duty of care to manage the records they create or use responsibly and adequately
- Information must be managed to support business functions
- Records should be held in a managed system and should be accurate, up to date and accessible
- Records must not be retained, distributed or copied unnecessarily
- A consistent approach must be adopted with regard to the creation, indexing, storage, retrieval, revision, archiving and disposal of records
- The management of information must be in accordance with security, protection, legal, environmental, and cost requirements

6. Definitions

Corporate Records	Records of business processes such as accounting, procurement, staff management and estates maintenance.
Data Protection Act	Data Protection Act 2018. UK legislation implementing the UK General Data Protection Regulation (UK GDPR). Everyone responsible for using personal data must comply.
Data Subject	An individual who is the subject of personal data.
Information Governance	An umbrella term relating to the processes and systems used by organisations to manage the information they hold; specifically refers to the processes and procedures used to ensure confidentiality, security, and accuracy of information.
Information Life Cycle	A term that describes a controlled regime in which information is managed from the point when it is created to the point when it is either destroyed or permanently preserved as being of historical or research interest.
Metadata	Data that describes information about other data, e.g., author and creation date of a record are elements of its metadata.
Permanent preservation	A process followed to place a record in an archive storage location allowing public access to records of historical administrative or local importance.
Public Authority	An organisation within the categories listed in Schedule 1 to the Freedom of information Act defined as ‘a body that appears to be exercising functions of a public nature or who are providing, under contract with a public authority, any service whose provision is a function of that authority. Optalis is a Public Authority by virtue of its ownership by two Local Authorities.
Public Records	Administrative and departmental records belonging to Her Majesty, in the UK or elsewhere, in right of Her Majesty’s Government, and in particular records of or held in any government department and records of offices, commissions or other bodies under HMG in the UK. (Public Records Act 1958). All Optalis records are public records subject to the Public Records Act (1958)
Record	A record is content that documents a business transaction. Documentation may exist in contracts, memos, paper files, electronic files, reports, emails, videos, instant message logs or database records.

Record appraisal	The process of deciding what to do with a record when the business use has ceased. The outcome of record appraisal will be either: destroy/delete, retain for a further period or transfer to a Place of Deposit.
Record Classification Scheme	Means by which a record-keeping system arranges or organises records to enable appropriate management controls to be applied and support accurate retrieval of information, e.g., a filing index
Record closure	The process followed to make a record inactive when it has ceased to be in active use other than for reference purposes.
Record Disposal	The destruction, deletion or transfer for permanent preservation of a closed record
Record retention	The process of keeping a record for a period for administrative, legal, fiscal, historical, or other purposes.
Records Management	Records management (RM) is the supervision and administration of digital or paper records, regardless of format. Records management activities include the creation, receipt, maintenance, use and disposal of records.
UK General Data Protection Regulation (UK GDPR)	Based on the European Regulation, the UK GDPR came into force from 01 Jan 2021 with the completion of Brexit. Combined with the Data Protection Act 2018, it forms the main data protection legislation for the UK.

7. Regulatory and Legal Framework

Under the terms of the Public Records Act all records created in Optalis are regarded as public records. The act imposes a statutory duty to make arrangements for the safe keeping and eventual disposal of records. The ownership and copyright of records created within Optalis lies with the company and not the individual who has created them.

As a Public Authority (due to the nature of our business and our local authority shareholders) subject to the Freedom of Information Act Optalis has a **duty** to follow the Code of Practice for Records Management in accordance with Section 46 of the FOIA. The code provides guidance to public authorities on keeping, managing and destroying records.

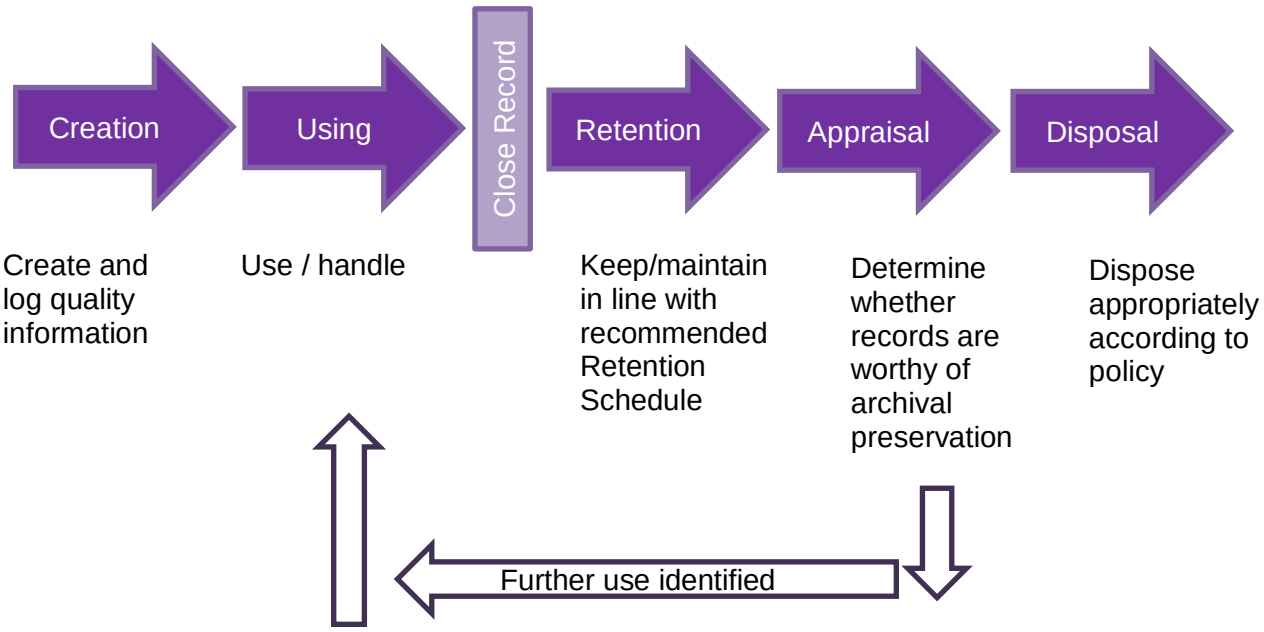
The Data Protection Act sets in law how personal and sensitive information may be processed and largely influences the way we handle care records. Further guidance on the confidentiality aspects of record-keeping is provided in the Confidentiality Code of Practice and Optalis' **OPS13 Data Protection Policy**.

The Records Management Code of Practice for Health and Social Care 2016 provides records management guidance for NHS and Social Care organisations based on current legal requirements and professional best practice. Optalis is committed to following the guidance issued in the code of practice and the procedures outlined in this policy are largely based on the guidance included in this Code of Practice.

8. Records Information Lifecycle

The Records/Information Life Cycle describes a design of flow to ensure information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. The details of this requirement can be read within policy **OPS61 Record Retention and Destruction**. The cycle is illustrated in figure 1, below:

Figure 1. The Information Lifecycle



Record Creation; ISO 15489-1:2016 Information and Documentation - Records Management describes the characteristics of 'Authoritative Records' as being authentic, reliable integral and useable, which the table below expands upon:

Record Characteristic	How to Evidence
Authentic	It is what it purports (claims) to be. It was created or sent by the person purporting to have created or sent it; and It was created or sent at the time purported.
Reliable	Full and accurate record of the transaction/activity or fact. Created close to the time of transaction/activity. Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	Complete and unaltered. Protected against unauthorised alteration. Alterations after creation can be identified, as can the persons making the changes.
Useable	Able to be located, retrieved, presented, and interpreted The context can be established through links to other records in the transaction/activity.

9. Creating, Handling and Using Records

When completing entries in or creating any form of records, the following general guidance should be applied:

- Be factual, consistent, and accurate
- Write clearly and in such a way that text cannot be erased
- Write in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read

Rights granted to members of the public by the Freedom of Information Act and to customers and staff under the Data Protection Act can result in copies of **corporate records being placed in the public domain and data subjects obtaining copies of records containing information about them**. On the basis that record entries are factual and accurate and personal records do not include any unnecessary and/or derogatory comments, record disclosure should not create any additional issues.

Accuracy

Good management of records ensures the user has confidence in the validity and accuracy of the information. The creation of supporting data about the record (metadata) establishes a records context and its place in time. The established standards for minimum metadata requirements are broadly as follows:

- Author/creator
- Record title
- Subject and keywords
- Description
- Date of creation and (if necessary) of any transaction relevant to the record's authenticity

- Format (electronic records must be retained in a format that enables them to be preserved with the structure intact (including layout, formatting and other elements)). The format should be retained when migrating to new software environments

  Records series association. Records need to be kept in orderly folders containing associated information. Sufficient information must be given in the naming and structure of the information to allow records to be understood when they are retrieved. Major records series (e.g. Personnel Records) will feature in the Retention Schedule.

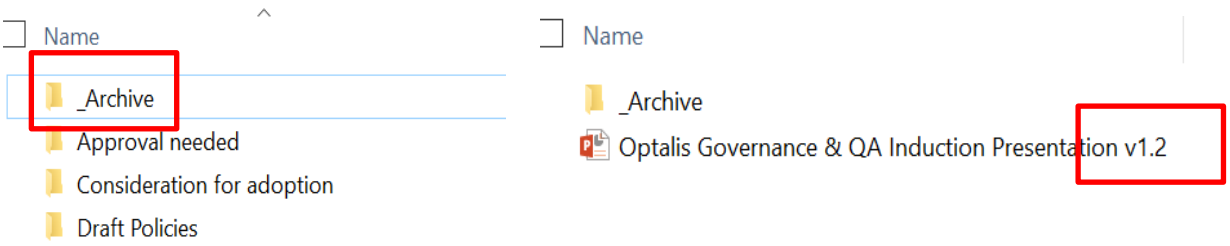
  Version Control (this is set at the end of a document title in the format of v0.1 as a starting point, and incremental for minor changes, whereas V1 or V2 etc. show a major change within the document, and by using this format will always show the latest version first)

  Security Marking should be used where appropriate

  The links between records, which document a sequence of activity, must be preserved. For example, an electronic mail message that is a reply to a previous one should contain the previous message or a reference to it

  Emails should not cover a number of different topics in the same message. A single topic should be covered within one email conversation. Multiple topics can cause confusion and result in different responses to the different topics contained in the conversation

All Optalis records should be stored within an appropriate filing system after creation. This will ensure they remain secure and accessible from the outset and be available to support the company's business activity, which can be undertaken by assuring appropriate levels of access to and within directories and through the use of suitable archiving and structuring, as shown below:



Confidentiality and Access

All Optalis records are public records and are subject to several statutory provisions regarding confidentiality, access, and disclosure. Optalis are trusted by customers and staff to treat their information respectfully, confidentially, and within the confines of the law. To ensure legal requirements are met, it is essential that Optalis provides, and is seen to provide, a confidential service.

Specific guidance on confidentiality issues is provided in both the Data Protection Policy and the Information Security Policy. Further advice on all aspects of confidentiality and the application of the Data Protection Act (2018) about the way we handle records in Optalis can be obtained from the Data Protection Officer (dpa@optalis.org).

The Act makes provision in law for 'data subjects' (e.g., customers and members of staff) **to obtain copies or otherwise gain access to information held about them**.

The Freedom of information Act 2000 provides members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of **this legislation is to make it possible for people to obtain copies of a wide range of Optalis records that in the past would have remained confidential**. The Freedom of Information Policy covers this aspect of records management and further advice on the procedure can be obtained from the Data Protection Officer.

Record Tracking

Ideally, the movement and location of all records should be controlled to ensure that a record can be retrieved at any time and there is an auditable trail of record transactions. This is best achieved using some form of record tracking system to record the movement of records between locations. It is the policy of Optalis that record folders are tracked using relative mediums and platforms such as iTrent, Agresso, Mosaic or Paris, as relevant. Users are provided with training to use the system(s) prior to being granted access directly. While electronic records do not require tracking as such, control must be exercised when hard copies are produced. If separate case notes are produced from electronic systems to form a filing system, individual record movements should be tracked to aid retrieval and avoid loss of data. For most areas, where the movement of records is **restricted**, paper-based systems may be employed, using registers to record the relevant information.

Record Storage

When not required for operational purposes, records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area, in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. Optalis do this through a national company called Iron Mountain, and each Service Manager or agreed appropriate delegate is provided with unique access details for this requirement to be carried out. Iron Mountain ensure that each user's access shows a comprehensive record of any records sent for commercial storage including a proposed date for review/destruction.

Digital information should be stored in such a way that throughout the lifecycle it can be recovered in an accessible format. Over time such changes as migration to new formats can cause links to other documents and embedded documents to fail to open impacting the integrity of the record. Any changes to the electronic storage systems used to hold Optalis records should only take place after full consideration of the impact on the records held and successful testing of retrieval of transferred records from the new version/system; evaluated through a Data Protection Impact Assessment (DPIA).

For assistance with conducting a DPIA please contact the Data Protection Officer.

Record Closure and Retention

A record should be closed when the business use for that record ceases. Following closure, records are subject to a minimum period of retention. The length of the retention period varies by record type and is based on legal and regulatory requirements and the assessed importance of and likely need to access the type of record.

Certain types of corporate records (e.g., finance, meeting records etc.) will follow annual cycles with existing records closed following year-end and new records created for the new year (calendar or financial), as described within the **OPS61 Record Retention Destruction Policy**.

10. Additional Guidance on Specific Record Types

E-Mail

Personal e-mail accounts tend to be structured according to personal preference and the data stored is not searchable and organised in a systematic way, making e-mail accounts unsuitable for record storage purposes. E-mail accounts should not be used to file records permanently but should be regarded as **transient storage areas** for working documents. E-mails or documents distributed by e-mail that need to be retained as Optalis records should be copied to the appropriate paper or electronic registered file system and the e-mail copy destroyed as soon as practicable. Where email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral, e.g., an email approving a business case must be saved with the business case file. Emails that are the sole record of an event or issue, for example an exchange between staff and a customer, should be copied in to the relevant record rather than being simply deleted. Email subjects should be appropriate and accurate to ensure expedience of search and navigation.

Scanned Records

Where paper records are scanned, the main consideration is that the information can perform the same function as the paper counterpart did, and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.

Complying with the standard, 'BS10008 Evidential Weight and Legal Admissibility of Electronic Information *(now BS10008:2014 due to revisions against upgrades with technology)'* provides one method of ensuring and demonstrating that electronic information remains authentic. The scanning of customer records for inclusion in Mosaic, Paris, iTrent or Agresso is being carried out in accordance with this standard. For smaller-scale local record scanning projects, compliance with the full scope of BS1008 will not be the appropriate methodology.

Methods that can be employed to ensure that scanned records can be considered authentic include:

- A written procedure outlining the process to scan, quality check and any destruction process for the paper record
- Evidence that the process has been followed
- An audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- Fix the scan into a file format that cannot be edited such as Portable Document Format (PDF)

Duplicate Records

Within any record-keeping system, there is a primary instance which can be considered the version that needs to be kept and this will normally be held by the person or the team with the function to provide the service or activity about which the records relate. It is not necessary to keep duplicate instances of the same record unless it is used in another process and is then a part of a new record. An example of this is incident forms. Once the information is transcribed into the incident management system, there is no longer a need to hold the (now) duplicate instance of the original form used to record the incident. There may be some local exceptions to this practice with appropriate justification.

Care or Health Records of Transgender Customers

A customer can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time, a new NHS number can be issued, and a new record can be created, if it is the wish of the customer or member of staff. Except in a limited set of circumstances, it is an offence under the gender recognition act to disclose without consent information that would identify that a person has undergone a gender identity change.

The key to the successful management of records in these circumstances is to discuss choices with the customer or staff member and agree what they wish to happen with respect to their record. If a new record is being created there is a need to identify which records are moved into the new record and to discuss how to link any records held in

any other institutions with the new record.

11. Roles and Responsibilities

Chief Executive

As accountable officer the Chief Executive Officer (CEO) is responsible for the overall leadership and management of Optalis and its performance in terms of service provision, financial and corporate viability, ensuring that Optalis meets all its quality and safety, statutory and service obligations and for working closely with other partner organisations. The CEO delegates aspects of this responsibility to relevant Directors according to their remits and accountabilities.

Head of Finance, Compliance & Performance

The Head of Finance, Compliance & Performance is the appointed Manager with responsibility for overall Information Governance including records management.

SIRO – Senior Information Risk Officer

The SIRO is responsible for managing information risk in Optalis and will implement and lead the Information Governance risk assessment and management processes within Optalis and advise the Board on the effectiveness of information risk management.

Caldicott Guardian

The Caldicott Guardian is the person who has a particular responsibility for reflecting patients' interests regarding the use of person identifiable information. The Caldicott Guardian is responsible for ensuring customer identifiable information is shared in an appropriate and secure manner.

Information Governance Officer

The Information Governance Officer is responsible for ensuring that this policy is implemented and that the records management system and associated processes are developed, coordinated, and monitored. The Information Governance Officer is also responsible for the overall development and maintenance of records management practices and promoting compliance with this policy in such a way as to ensure the easy, appropriate, and timely retrieval of customer information.

Head of Service Managers

The responsibility for local records management is devolved to services and Heads of Service who retain overall responsibility for the management of records generated by their activities. I.e., for ensuring that records created within their service are managed in a way that meets the aims of our records management policy and associated procedures.

Service Managers

All Managers have a responsibility to ensure all staff they manage are adequately trained in record-keeping and are aware of and adhere to the standards for record-keeping outlined in this policy.

All Staff

Members of staff who create, receive and use records have records management responsibilities. In particular, all staff must ensure that they keep appropriate records of their work in Optalis and manage those records in keeping with this policy and with any guidance subsequently produced. Staff who make entries in records should do so in accordance with the record-keeping standards published in this policy.

12. Contemporaneous Notes

Contemporaneous Notes are notes made at the time or shortly after an event occurs. They represent the best recollection of what you witnessed.

The following information clarifies the basis for making and keeping notes:

- Investigations into cases of alleged or actual abuse or neglect may in some cases lead to criminal and civil proceedings of one kind or another. E.g., investigators may be called as witnesses for the police in criminal proceedings or on behalf of regulatory bodies in connection with criminal and civil proceedings against registered providers
- Notes taken in the course of investigations for one purpose may be important in the context of giving evidence in legal proceedings. Notes taken at the time of meetings with individuals, telephone calls, visits to premises and so on are referred to as 'contemporaneous' notes
- The value of contemporaneous notes is greatly enhanced evidentially in criminal proceedings and would have to conform to Rules of Evidence and statutory Codes of Practice set out in the Police and Criminal Evidence Act 1984 (PACE)
    - The notes recorded should be: -
        - Factual – write nothing you would be unhappy to read out in court
        - Made in ink at the time of an event or as soon after as is reasonable and practical
        - Dated
        - Original and not copied from elsewhere

As memory is fallible, such notes may be the only place from where evidence can be recalled and substantiated, so the following points should be observed:

- No erasures
- No leaves to be torn out
- No blank spaces to be left
- No overwriting
- No writing between lines
- No separate pieces of paper
- Amendments to be initialled

This guidance does not constitute full adherence to the law and statutory Codes of Practice for the keeping of contemporaneous notes but will assist if staff are called to give evidence in legal proceedings.

13. HR Record-keeping

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The focal point of any staff file will be the paperwork collected through the recruitment process and this will be expanded over time with additional material added by line managers. To reduce the burden of storage a summary record may be prepared and held.

Human Resource records cover a wide range of personal and organisational documents and data which are typically stored as computer or paper files. It is important that Optalis has effective systems for the collection, access, storage and destruction of this information to ensure it remains compliant with all relevant legislation and to support sound and effective HR practice and administration. All HR records have a unique identifier in their employee number.

The guidance and practice contained in this document applies to all staff at all times and **failure to follow it may result in disciplinary action**. The Data Protection Act 2018 (DPA) applies to information about living, identifiable people and so most HR records would fall under this Act regardless of the media used for information storage.

Employee records are an essential resource in order for Optalis to demonstrate:

- Compliance with statutory and regulatory standards in all stages of employment
- Compliance with statutory responsibilities in checking an individual's eligibility to work in the UK
- Audit trails to provide assurance of currency of professional registration
- Accuracy and currency of data held in relation to individual employees
- Compliance with statutory requirements and best practice in:
    - Recruitment and selection
    - Equality
    - Health and safety
    - Management of workplace disputes
    - Management of capability / discipline / conduct
    - Training provision / CPD
    - Equal Pay
    - Data Protection Act

In each of these areas, the information collected (including that collected at the interview) must be relevant and not excessive and respect the employees' right to a private life. Information (including that collected at the interview) must be recorded accurately and only be kept for as long as is necessary. The employee must be aware of the reasons for the information being collected and any information collected 'covertly' about the employee, for whatever purpose, is likely to breach the Data Protection Act (DPA). Consult the Data Protection Officer if you need advice about covert recording.

This encompasses all files and records that include personal data relating to individual employees and may include Personnel files created at the point of appointment, Health and Safety records, including compliance with Working Time Directive, Training records including statutory continuous professional development and Incident and issues "Case files" for example:

- Misconduct
- Sickness absence

- Performance / capability issues
- Individual grievances / disputes

The Information Commissioner's Office identifies in its guidance four key areas of HR record-keeping and practice, they are:

- Recruitment and Selection
- Employment Record
- Monitoring at Work
- Information about Workers Health

In addition to supporting HR to maintain and update their information the Line Manager also has specific responsibility for the following day to day information gathering, recording, and monitoring.

All staff must ensure that any changes in their personal circumstances or personal information are notified without delay to their manager to ensure currency and accuracy of data is maintained at all times.

All staff identified as having legitimate access to records must receive training in Data Protection legislation and associated aspects of records management. All staff and managers have a duty of care when handling and using personal data. Information held on individuals must not be passed to any person or body with no legitimate interest in it.

Data must be kept secure at all times. Lockable storage must be provided for paper documents. Electronic files must be password protected or stored on drives accessible only to authorised personnel. Under no circumstances should files /records be allowed off-site or outside of Optalis without written authority of the Head of Service or Director of HR. Confidentiality must be maintained at all times. Personal information **must not** be released without the employees express knowledge and consent unless there is overriding public interest.

HR documents may be required for a number of reasons, one being Employment Tribunal or other legal action where there is an expectation that the original documents are available. It is therefore vital that documents are properly stored throughout their 'life' and are not lost or damaged by storage in damp conditions or when computer equipment is upgraded.

Where information is deliberately destroyed in line with this guidance an accurate record must be kept of the reasons why, when, and how this was done. The employer may be required to provide a 'statement of truth' for any legal action and failure to provide a full explanation of why the original documents are no longer available may injure the employers' case.

14. Customer Care Record-keeping

Care records include any record which is made in the context of care provided by Optalis to individuals or families, e.g., daily logs, reports and assessments, in whichever form they may be created, whether by hand or electronically. As a care provider Optalis is bound by legislation and regulation in its day-to-day operations and in line with our vision, mission and values aspire to always be person-centred in the way that care records are written. Being person-centred means having regard to the dignity of the customer at all

times, ensuring that records are written respectfully. The person creating the record should be confident that they would be satisfied to read a similar record in relation to themselves or a loved one. With the customers consent, records should include:

- Assistance with medication including time and dosage
- Financial transactions undertaken on behalf of the customer
- Details of any changes in the customer's or carer's circumstances, health, physical condition or care needs
- Any accident, however minor, to the customer and/or care or support worker
- Any other information that would assist the next health or social care worker to ensure consistency in the provision of care
- All records required for the protection of customers and for the effective and efficient running of the organisation should be maintained in an up-to-date and accurate fashion by all staff
- Customers have access to their records and information about them held by the organisation; they are also given opportunities to help maintain their personal records at initial assessment, reviews, and other occasions
- Individual records and company records are kept securely; are up to date and in good order; and are constructed, maintained, and used in accordance with the Data Protection Act (DPA) 2018 and other statutory requirements
- Ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff who have a need and a right to access them
- Ensure that all files or written information of a confidential nature are not left in a place where they can be read by unauthorised staff or others

15. Financial Record-keeping

Accurate record-keeping is imperative for Finance, and financial records should hold sufficient information about all relevant activity relating to Optalis. The volume of information collected and processed will expand over time with additional information or changes to current information as a natural part of the business functionality. To reduce the burden of storage a summary record may be prepared and held.

Financial records are largely held electronically through the Agresso system, which is widely used across both Optalis and its partners, and it is important that Optalis has effective systems for the collection, access, storage, and destruction of this information to ensure it remains compliant, secure with all the relevant legislative requirements and effective in practice and administration. All financial records have a unique reference in their association with the following:

- Monitor the progress of business
- Annual Plan; 3yr performance projections and current year
- Tax liabilities and returns
- Financial statements and Expenditure

- Purchasing and Invoicing
- Insurances
- Budgets and deficits
- Creditors and Debtors
- Profit and Loss Account
- Audit and Review
- Tenders and new work
- Contracts, Service Level Agreements, and their Schedules
- Any financial irregularities
- Assurance of 'Good Governance'
- Delegated powers
- Gifts and Legacies
- Handling of Money, Customers Lacking Capacity
- Loss or damage to the assets of the business
- Any evidence of fraud or criminal activities

The need for good record management is of critical value to monitor the progression of Optalis, the successes, contractual obligations, legislation compliance and any/all implemented changes agreed. Failure to manage records in a proper manner could severely damage Optalis' reputation.

16. Access to Records

The rights of an individual (otherwise known as a data subject) to access personal information and records held by Optalis are set out in the UK GDPR. People whose personal information is held in any form have a right of access to the information; this is known as a Data Subject Access Request (DSAR).

The right of access applies to both paper/hard copy records and records held electronically. When someone requests **all** of their information this may include formal records held in a system (e.g., Paris / Mosaic, iTrent (employee information)), emails relating to them, any information on spreadsheets or Word documents, and printed files. Once a request is received the information cannot be altered or changed in any way; this is one reason why it is vital that records are written and maintained professionally.

The Freedom of Information Act 2000 gives access to non-personal information held by public authorities. Under the Act, anybody may request information in writing, via e-mail or even a verbal request from a public authority (which includes all local authorities) and must receive a response within 20 working days.

Any 'confidential' data should be clearly labelled and include staff who have the right to access the information. **However, it must be understood that marking documents or emails as 'confidential' does not necessarily mean that they are considered confidential under either the UK GDPR or Freedom of Information Act. Therefore,**

information labelled as 'confidential' within Optalis may still be released to the individual involved or to the public as required. E.g., an email to the CQC asking for advice about a situation in a care home and marked 'confidential' is likely to be released (although any personal data may be removed).

17. Risk Management

Efficient records management enables Optalis to manage risk and thus:

- Reduce the number of incidents in business continuity and business-critical areas due to not being able to find core records
- Reduce the risk of not being able to use the records as legal submissions
- Reduce the risk of not meeting statutory requirements
- Prevent unauthorised access to restricted data confidential information

18. Training Statement

All staff must read this policy and related policies on data protection, access to records and information security on an annual basis to understand the current policy and practice. Training in the correct method for entering information in customers' records will be given to all staff.

19. Related Policies

WBC 706 Access to Restricted Social Care Records

Berkshire Adult Safeguarding Policies and Procedures

Mosaic Policies – WBC

Paris Guidance is available from RBWM

OPS11 Care and Support planning

OPS13 Data Protection Policy

OPS29 Information Security

OPS30 Information Sharing Protocol

OPS61 Record Retention Destruction

20. References

BS10008 Evidential Weight and Legal Admissibility of Electronic Information (now BS10008:2014 due to revisions against upgrades with technology)

Code of Practice on the Management of Records; Section 46 of the Freedom of

Information Act (2000).

Companies Act 2006

Data Protection Act (2018)

Finance Act 2013

Financial Services and Markets Act 2000

Freedom of Information Act (2000)

General Data Protection Regulation

Health and Safety at Work Act 1974

Income Tax (PAYE) Regulations 2003

International Standard on Records Management, BS ISO 15489

Limitation Act 1980

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019

Sanctions and Anti-Money Laundering Act 2018

Pensions Act 2008

Public Records Act (1958)

Records Management Code of Practice for Health and Social Care 2016

Social Security (Contributions) Regulations 2001

Statutory Sick Pay (General) Regulations 1982

Taxes Management Act 1970

Value Added Tax Act 1994

21. Contact

Data Protection Officer
Email: dpa@optalis.org

Trinity Court
Molly Millars Lane
Wokingham, RG41 2PY