Verilife

DATA PROTECTION - CUSTOMER AND CLIENT NOTICE

SMITHFIELD HEALTH & SOCIAL CARE LTD | 363 SOUTHBOROUGH LANE, BROMLEY BR2 8BQ

PART ONE
ABOUT THE POLICY

OVERVIEW

Smithfield Health and Social Care Limited, trading as Verilife ('the Company, us, we, our'), takes the security and privacy of your data seriously.

We must gather 'personal data' (information) about you as part of our business and manage the care services we provide for/to you. We intend to comply with our legal obligations under the **UK Data Protection Act 2018** and the **UK General Data Protection Regulation (UK GDPR)** regarding data privacy and security. We must provide you with the information set out in this policy.

This policy applies equally to our Customers and **Clients** ('you'), but not all sections are relevant to both groups.

Our '**Customers'** are persons or organisations that pay for the care services we provide our Clients.

Our '**Clients'** are persons who receive the care services we provide.

Clients may also share information about their care stakeholders—those who assist in their care, such as family members, friends, neighbours, and personal assistants. If applicable under data protection law, this notice also covers these individuals.

If you fall into one of these categories, you are a '**data subject**' for this policy.

This notice explains how the Company will hold and process your information and outlines your rights as a data subject.

The Company is a **data controller**, meaning we determine how to process your personal data. Processing personal data includes collecting, storing, using, recording, altering, structuring, correcting, restricting, disclosing, transferring, or destroying it.

Additionally, we may act as a **data processor** on behalf of our Customers, storing and updating information provided in regard to their clients.

PART TWO
DATA PROTECTION PRINCIPLES

DATA PROTECTION PRINCIPLES

We will process personal data in line with six **Data Protection Principles**:

- Processed fairly, lawfully, and transparently.
- Collected and processed only for specified, clearly explained, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Not kept for longer than necessary.
- Processed securely.

We are **accountable** for these principles and must demonstrate compliance.

HOW WE DEFINE PERSONAL DATA

'Personal data' means **information relating to an identifiable person**, either on its own or when combined with other information. Examples include:

- Contact details, date of birth, gender, and marital status.
- Emergency contact details.
- Medical history and care records.
- Identification documents (e.g., passport, driving licence, immigration status).
- CCTV images, photographs, or video recordings.

We also process **special categories of personal data**, including information on **health, race/ethnicity, religious beliefs, genetic/biometric data, and sexual orientation**, in line with legal requirements under **Article 9(2) of the UK GDPR**.

HOW WE DEFINE PROCESSING

'Processing' includes:

- Collection, recording, and storage.
- Adaptation, alteration, retrieval, and consultation.
- Use, disclosure, alignment, or combination.
- Restriction, destruction, or erasure.

CATEGORIES OF DATA WE COLLECT

We capture the following data sets about a service user:

- **Personal identification data** — Name, contact details, DOB, identified gender, ethnicity, etc.
- **Stakeholder details** — include LPA holders, NOKs, family members, GPs, client support networks, etc.
- **Billing and Financial Information** — Commissioner details, bill payment information, and payer details.
- **Health and Wellbeing Data** — Mental capacity, medical conditions, mental health, disabilities, injuries, life and medical history, care needs, domestic needs, medication, nutrition and hydration needs, mobility status, etc.
- **Care and Support Preferences** — Best interest decisions, care delivery preferences, care goals, EOL preferences and wishes, etc.
- **Communication Records** — Communication with professional services such as the client's GP, commissioners, etc.
- **Service Delivery Environment** — Information about the environment where services are provided.
- **Consent Documentation** — The service user or their legal representative obtained various consents.
- **Risk and Care Management** — Risk assessments, Care and Support Plans.

- **Operational Data** — Visit logs, care notes, invoices and other records necessary for service provision.

WHY WE PROCESS YOUR DATA

We process your data to:

- Comply with **legal and regulatory obligations**.
- Perform our **contractual obligations** to customers.
- Deliver **safe and effective** care to our clients.
- Pursue our **legitimate interests**.

- **Personal identification data** (Name, Contact Details, DOB…)

  Why? To correctly identify the service user, maintain accurate records, and ensure communication with the right individual for care and legal purposes.

- **Stakeholder Information** (LPA Holders, NOK, Family Members…)

  Why? To contact key stakeholders for decision-making, care coordination, and emergencies. This includes obtaining input for care decisions and liaising with medical professionals.

- **Billing and Financial Information** (Commissioner, Bill payer…)

  Why? To process payments, manage contracts, and ensure compliance with funding requirements for care services.

- **Health and Wellbeing Data** (Mental Capacity, Disabilities…)

  Why? To assess the service user's needs and provide safe, appropriate, and legally compliant care tailored to their health conditions and capabilities.

- **Care and Support Preferences** (Best Interest Decisions…)

  Why? To provide **person-centred care**, respect the individual's choices, and fulfil legal and ethical obligations in decision-making, including end-of-life care.

- **Communication Records** (Client's GP, District Nurses...)

  Why? To ensure that relevant medical and care professionals are kept informed of the service user's condition and changes in care needs.

- **Service Delivery Environment** (Service delivery environment...)

  Why? To conduct **risk assessments**, ensure **safe working conditions**, and adapt care plans based on the home environment.

- **Consent Documentation** (Consent to Care...)

  Why? Record **legal permission** for processing data, providing care, sharing information with stakeholders, and delivering medical interventions.

- **Risk and Care Management** (Risk Assessments, Care Plan...)

  Why? To **identify potential risks**, prevent harm, and comply with health and safety regulations in domiciliary care settings.

- **Operational Data** (Visit Logs, Care Notes...)

  Why? To track service delivery, ensure compliance with care plans, and maintain accurate records for audits, legal purposes, and quality assurance.

SHARING YOUR DATA

We may share your data with:

- **Care professionals and medical providers** involved in your care.
- **Regulatory bodies** (e.g., CQC, NHS, ICO) to comply with legal duties.
- **Law enforcement agencies**
- **Commissioner** of your care or other contracted parties.
- **Service providers** that support our business.

Data will not be transferred outside the **European Economic Area (EEA)** unless appropriate safeguards are in place.

HOW WE HANDLE DATA BREACHES

We have strict security measures to prevent data breaches. If a breach occurs, we will:

- Investigate and **document** the incident.
- **Report to the ICO within 72 hours** if required.
- Notify affected individuals or organisations where necessary.

PART THREE
RIGHTS AND DATA SECURITY

YOUR RIGHTS AS A DATA SUBJECT

You have the right to:

- **Right to be Informed** — You have the right to be informed about how your personal data is used, including how long we keep it and who it is shared with.
- **Right of Access**—You can request a copy of the personal data we hold about you via a SAR request.
- **Right to Object** — If you do not want us to use your data, you can object and ask us to stop processing or sharing it unless there is a legal reason to continue.
- **Right to Rectification** — If any personal data we hold is inaccurate, you have the right to ask us to correct it without undue delay.
- **Right to Erasure** — You can request that we delete your personal data, and we must do so unless there is a legal or operational obligation to retain it.
- **Right to Restrict Processing** — In certain circumstances, you can request that we limit how we process your data, such as if you challenge its accuracy or object to processing.
- **Right to Data Portability** — You can ask us to transfer your data to another provider in a structured, commonly used, and machine-readable format.
- **Be notified of security breaches** that may affect your rights.

EXEMPTIONS TO GDPR RIGHTS

There are situations where some GDPR rights may not apply, including:

- **Legal Obligation** – If we are legally required to retain certain data, the Right to Erasure may not apply.
- **Public Interest** – If data is required for public health, scientific research, or statistical purposes, the Right to Object may not apply.
- **Legal Claims** – The Right to Restrict Processing may not apply if data is needed for legal proceedings.

SUBJECT ACCESS REQUEST (SAR)

A **Subject Access Request (SAR)** is a request made by an individual to access the personal data that an organisation holds about them. This is a right under the **UK GDPR and Data Protection Act 2018**.

How to Make a SAR:

1. **Format of Request** – A SAR can be made **in writing, via email, or verbally**.
2. **Details to Include** – The individual should provide:
    - Their **full name and contact details**.
    - The **full name** of the person they request data on – the data subject (if not themselves).
    - A **clear description** of the information they want to access.
    - Any **specific dates or context** to help locate the data.
    - The **basis for the request**.
3. **Verification of Identity** — The organisation may request proof of identity to confirm the requestor's identity before processing the SAR. If the requester is not the same as the data subject, Verilife will get confirmation from the data subject before releasing the information.
4. **Response Time** — Verilife will aim to respond within 30 working days of the request. If the request is complex, this can be extended by two more months.
5. **Fees** — A SAR is free, but we may charge a reasonable fee if the request is excessive, requires extensive processing, or is repetitive.

Verilife may refuse a SAR request or return a reduced data set if:

- **Manifestly unfounded** — The request has no valid basis or is intended to harass the organisation.
- **Nature of the Request** – The request is **unreasonably broad** or requires an **unreasonable fulfilment effort**.
- **Excessive or repetitive** — The same request is made multiple times without justification.

- **Proportionality** – The request **imposes a disproportionate burden** on the organisation compared to the individual's need for access.

Subject Access Requests can be made in writing to:

Stephen Smith
Data Protection Officer
Verilife
363 Southborough Lane, Bromley, BR2 8BQ
Email: **stephen.smith@verilife.co.uk**

DATA RETENTION AND DESTRUCTION

- Personal data is retained for the duration of care service provision.
- Data is generally held for six years after service termination to comply with legal obligations.
- Secure destruction or anonymisation is carried out at the end of retention periods

DATA SECURITY MEASURES

We comply with the **NHS Data Security and Protection Toolkit (DSPT)**, ensuring our data security meets NHS standards.

The technical and organisational safeguards in place, including:

- **Firewalls** between ourselves and the internet.
- **Encryption** and **access control measures**.
- **Regular security audits** and **system updates**.
- **Contractual safeguards with third-party data processors**.

PART FOUR
COMPLIANCE AND COMPLAINTS

ACCOUNTABILITY

We are committed to resolving any data protection concerns internally. If you have any complaints, please contact:

Stephen Smith
Data Protection Officer
Email: **stephen.smith@verilife.co.uk**

If your concerns remain unresolved, you have the right to complain to the **Information Commissioner's Office (ICO)**:

ICO Contact Details:
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 0303 123 1113
Website: www.ico.org.uk

PART THREE
APPENDICES

Appendix: Glossary of Technical Terms

- **Access Control** – Security measures ensuring that only authorised individuals can access certain data.
- **Anonymisation** – The process of removing personally identifiable information to prevent identification.
- **Consent** – The explicit permission an individual gives for their data to be processed.
- **CQC (Care Quality Commission)** – The independent regulator of health and social care in England.
- **Data Controller** – The entity that determines the purpose and means of processing personal data.
- **Data Processor** – A party that processes personal data on behalf of the Data Controller.
- **Data Subject** – An individual whose personal data is being processed.
- **Destruction** – The secure and irreversible deletion of personal data.
- **EEA (European Economic Area)** – Countries in which certain data protection laws apply.
- **Encryption** – A security method used to protect data by converting it into an unreadable format, accessible only with a decryption key.
- **ICO (Information Commissioner's Office)** – The UK's independent regulator for data protection.
- **NHS DSPT** – The NHS Data Security and Protection Toolkit, a standard for security compliance.
- **Personal Data** – Any information relating to an identified or identifiable individual.
- **Processing** – Any operation performed on personal data, including collection, storage, or deletion.
- **Retention Period** – The duration for which personal data is stored before being securely deleted.

- **Subject Access Request (SAR)** – A request made by an individual to access the personal data that an organisation holds about them.
- **Service Termination** – The end of a contractual relationship, triggering specific data retention and deletion rules.
- **Special Categories of Data** – Sensitive personal data, such as health, race, or biometric information.
- **UK GDPR** – The United Kingdom General Data Protection Regulation governing data privacy.