Privacy Policy

Effective Date: September 1, 2025]

Last Updated: September 1, 2025

HERE4YOU CARE LTD ("we," "us," or "our") is committed to protecting the privacy and security of personal data in accordance with applicable laws, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance from the Care Quality Commission (CQC). As a registered provider of health and adult social care services in England (Company Number: 15587616; Registered Office: 128 City Road, London, United Kingdom, EC1V 2NX; we handle personal data responsibly to deliver safe, effective, compassionate, and high-quality care while encouraging continuous improvement in our services.

This Privacy Policy explains how we collect, use, store, share, and protect personal data relating to individuals who use our services (service users), their families or representatives, our staff, contractors, and other stakeholders. It applies to all personal data processed by us, whether in electronic or paper form. We adhere to the principles outlined in the CQC's Code of Practice on Confidential Personal Information, the Caldicott Principles, and our internal Information Governance Policies to ensure ethical and lawful handling of information.

If you have any questions about this policy or our data practices, please contact our Data Protection Officer using the details provided at the end of this policy.

1. What Personal Data Do We Collect?

Personal data means any information relating to an identified or identifiable living individual. We may collect the following categories of personal data:

- **Basic Identification and Contact Information**: Name, address, date of birth, telephone number, email address, and emergency contact details.
- **Health and Care-Related Information** (Special Category Data): Medical history, care plans, medication records, health assessments, allergies, disabilities, mental health details, and records of care provided. This may include sensitive information such as racial or ethnic origin, religious beliefs, sexual orientation, or genetic/biometric data where relevant to care provision.
- **Financial Information**: Payment details, billing records, or funding sources (e.g., from local authorities or insurance providers).
- **Employment and Staff Data**: For our employees and contractors, this includes CVs, references, DBS checks, training records, performance reviews, and health declarations.
- **Feedback and Complaints Data**: Information provided in surveys, complaints, or feedback forms, including views on care received.
- **Monitoring and Safeguarding Data**: Records of incidents, safeguarding concerns, or interactions with other agencies.

- **Website and Digital Data**: If you visit our website or use our online services, we may collect IP addresses, browser types, and usage data via cookies (see our Cookie Policy for details).

We only collect data that is necessary for providing care, fulfilling regulatory obligations, or improving our services. We do not collect data for unrelated purposes.

2. How Do We Collect Personal Data?

We collect personal data through various lawful means, including:

- Directly from you or your representatives (e.g., during initial assessments, care planning, or ongoing interactions).
- From third parties with your consent or where legally required, such as GPs, hospitals, local authorities, or other care providers.
- Automatically through our systems (e.g., electronic care records or security monitoring).
- From public sources or regulatory bodies like the CQC, where relevant to our operations.

In line with CQC guidance, we obtain confidential personal information fairly and transparently, applying a 'necessity test' to ensure access is proportionate and justified (e.g., for inspecting care quality or responding to concerns).

3. Legal Basis for Processing Personal Data

We process personal data only where we have a lawful basis under the UK GDPR. Common bases include:

- **Performance of a Contract**: To provide care services as agreed in our service contracts.
- **Legal Obligation**: To comply with regulations such as the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, CQC requirements, or safeguarding laws.
- **Vital Interests**: In emergencies, to protect your life or health.
- **Legitimate Interests**: For internal administrative purposes, quality improvement, or staff training, provided this does not override your rights.
- **Consent**: Where appropriate (e.g., for marketing or sharing data beyond care needs), we obtain explicit, informed consent. You can withdraw consent at any time.
- **Public Task**: As a regulated care provider, to fulfill our role in protecting public health and safety.

For special category data (e.g., health information), we rely on additional bases such as explicit consent, provision of health or social care, or reasons of substantial public interest (e.g., safeguarding vulnerable individuals).

We follow the Caldicott Principles to justify the use of confidential information: (1) Justify the purpose; (2) Use only when absolutely necessary; (3) Use the minimum necessary; (4) Access on a strict need-to-know basis; (5) Be aware of responsibilities; (6) Comply with the law; (7) The

duty to share can be as important as the duty to protect; and (8) Inform patients and service users.

4. How Do We Use Personal Data?

We use personal data to:

- Deliver personalised care, including creating and reviewing care plans, administering medication, and monitoring health outcomes.
- Ensure compliance with CQC inspections and regulatory reporting (e.g., sharing anonymised data for quality monitoring).
- Handle complaints, incidents, or safeguarding concerns effectively.
- Communicate with you, your family, or representatives about care.
- Train staff and improve service quality through audits and reviews.
- Manage our operations, including billing, staffing, and risk assessments.

We do not use personal data for automated decision-making that significantly affects you without human oversight. All processing adheres to data protection principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.

5. Sharing Personal Data

We share personal data only when necessary and lawful, in accordance with our Code of Practice on Confidential Personal Information. Sharing may occur with:

- Healthcare professionals (e.g., GPs, hospitals) to coordinate care.
- Regulatory bodies like the CQC, local authorities, or safeguarding boards to protect individuals or comply with inspections.
- Emergency services in cases of serious harm or vital interests.
- Third-party processors (e.g., IT providers or auditors) under strict contracts ensuring data security.
- Other organizations for public interest purposes, such as public health inquiries (e.g., the UK Covid-19 Public Inquiry).

We do not share data for direct marketing without consent. Where possible, we anonymize or pseudonymise data before sharing. Disclosures are limited to special circumstances set out in law, and we maintain records of all sharing activities.

6. Data Security and Retention

We implement robust security measures to protect personal data, including:

- Encryption, access controls, and secure storage systems.
- Regular staff training on data protection and confidentiality.

- Incident response procedures for breaches, with mandatory reporting to the Information Commissioner's Office (ICO) and affected individuals where required.

Personal data is retained only as long as necessary, in line with our retention schedule (e.g., care records for 8 years after service ends, as per legal requirements). At the end of retention periods, data is securely deleted or anonymised.

7. International Transfers

If we transfer personal data outside the UK (e.g., to cloud providers), we ensure adequate safeguards are in place, such as UK International Data Transfer Agreements or adequacy decisions.

8. Your Rights

Under the UK GDPR, you have rights regarding your personal data, including:

- **Access**: Request a copy of your data.
- **Rectification**: Correct inaccurate data.
- **Erasure**: Request deletion in certain circumstances (e.g., if no longer needed).
- **Restriction**: Limit processing while concerns are addressed.
- **Objection**: Object to processing based on legitimate interests or public tasks.
- **Portability**: Receive your data in a transferable format.
- **Withdraw Consent**: Where processing relies on consent.

To exercise these rights, contact us using the details below. We respond within one month, free of charge (unless requests are excessive). If we hold your data and you object to its use, we will respect your preferences where possible, as per CQC guidance.

If dissatisfied, you can complain to the ICO (www.ico.org.uk).

9. Children and Vulnerable Individuals

For children or individuals lacking mental capacity, we involve parents, guardians, or representatives in data decisions, following Mental Capacity Act principles and ensuring best interests are prioritised.

10. Changes to This Policy

We review this policy regularly and may update it to reflect legal changes or service improvements. Updates will be posted on our website, and we will notify you of significant changes.

Contact Us

For questions, requests, or complaints about your personal data:

Data Protection Officer

HERE4YOU CARE LTD

128 City Road, London, United Kingdom, EC1V 2NX

Email:

Telephone: 07377113663

We are registered with the ICO [if applicable, insert registration number]. This policy aligns with our commitment to transparency and accountability as a CQC-regulated provider.