



Privacy Policy

Version 2.0





Our C.A.R.E. ethos has been designed in partnership with clinicians working in detention and supported by feedback from patients and charities that provide specialist support to represented groups.

Compassion: We recognise that people in secure environments are more likely to have experienced trauma and will naturally be worried and concerned. We ensure our staff are trained and supported to understand this and deliver compassionate and supportive care.

Assurance: Our Quality Assurance (QA) processes ensure that the services we deliver align with best practice standards and demonstrate high-quality outcomes for people under our care. We will also involve specialist charities through our innovative Third Sector Collective, to ensure we are reaching out into our communities/international partners & supporting people to reintegrate on release.

Respect: We respect and honour the diverse cultural and religious backgrounds of patients ensuring that our approach promotes equality and equity. People in our care are engaged in a way that is open and non-judgmental. By understanding their beliefs & practices, we can offer care that is sensitive to individual needs, fostering a sense of trust and promoting effective communication for better health outcomes.

Empowerment: All residents are placed at the centre of their care with our services sequenced around their specific and holistic care needs. Patients co-create care plans that are designed to treat their presenting conditions and empower them to self-manage, taking control of their wellbeing.

Table of Contents

Document Control	4
Document Revision History	4
1. Introduction	5
2. Who Are We	5
3. Data We Collect	5
Personal Identifying Information	5
Professional Data	5
Health Information	5
Compliance Data	5
Financial Data	6
Children's Data	6
4. How We Use Your Data	6
Fulfil Contractual Obligations	6
Manage Employment and Contract	6
Legal Compliance	6
Communication	6
Quality Assurance and Service Improvement	6
Safety and Security	6
5. Legal Basis for Processing	6
Performance of a Contract	7
Legal Obligation	7
Legitimate Interests	7
Special Category Data	7
Data (Use and Access) Act 2025	7
6. Sharing Your Information	7
Healthcare Facilities	7
NHS Trusts and Private Healthcare Providers	7
Regulatory Bodies	7
Third-Party Service Providers	7
Legal Authorities	7
International Transfers	8
7. Data Security	8
8. Retention of Data	8
9. Your Rights	8
Right to Access	8

Right to Rectification	8
Right to Erasure.....	8
Right to Restrict Processing	9
Right to Data Portability	9
Right to Object	9
10. Cookies and Website Usage	9
11. Changes to this Privacy Policy.....	9
12. Contact Us.....	9
13. Jurisdiction	9
14. National Data Opt-Out.....	9

Document Control

Version	2
Date Approved	June 2026
Approved By	Farwa Pasha
Review Date	June 2027

Document Revision History

Version	Date	Author	Version Approved By	Comments
2.0	June 2026	Operations	Farwa Pasha	Confirmed that the Data Controller wording is accurate for all categories of data, particularly clinical/patient data within secure-estate services. Confirmation that the lawful bases and Article 9 special category conditions align with the Record of Processing Activities, DPIAs and any Appropriate Policy Document Confirmed that the third-party supplier wording can be evidenced through supplier contracts, data processing agreements and due diligence records Confirmed that the retention wording matches the organisation's retention schedule, especially for employment, clinical, safeguarding and incident-related records; National Data Opt-Out wording reviewed to ensure it accurately reflects the processing undertaken by DrPA;

1. Introduction

At DRPA Secure, we are committed to protecting the privacy and security of our candidates, clients, healthcare practitioners, and other users. As a UK-based healthcare solutions provider for Immigration Removal Centres, Prisons, and other secure establishments, we comply with the General Data Protection Regulation (GDPR) and UK data protection laws. This Privacy Policy explains how we collect, use, store, and disclose your personal data.

We also comply with the Data Protection Act 2018, the Data (Use and Access) Act 2025, the NHS Data Security and Protection Toolkit (DSPT), the National Data Guardian Standards, and the NHS Records Management Code of Practice.

DRPA Secure acts as a Data Controller for the personal data of our candidates, employees, self-employed contractors.

DRPA Secure's status as Data Controller, Joint Controller, and/or Processor for clinical and patient data will be confirmed against the relevant NHS Trust, Home Office and secure-estate contracts and data-processing arrangements where applicable and appropriate.

2. Who Are We

DRPA Secure is a healthcare provider delivering medical services to secure establishments, including prisons, Immigration Removal Centres, and Young Offender Institutions within the UK. We work closely with the Home Office, NHS Trusts, and private healthcare providers.

3. Data We Collect

We collect and process personal data to deliver our services effectively. This includes:

Personal Identifying Information

Full name, date of birth, address, and contact information (email, phone).

Professional Data

CV details, job titles, work experience, qualifications, and employment history.

Health Information

Medical history, occupational health information, fitness-to-work assessments and safeguarding information, where necessary to provide healthcare services, comply with legal obligations, or as part of employment health checks.

This includes special category data processed under UK GDPR Article 9 for the provision of health care and employment-related purposes.

Compliance Data

Proof of right to work in the UK, DBS checks, and records required to comply with NHS and private contracts.

We may also process vetting and security information required by the Home Office, HMPPS, NHS Trusts and other secure-estate partners to ensure the safety and security of the environments in which we operate.

Financial Data

Bank account details, payroll information, and tax details (for employees and self-employed contractors).

Children's Data

Where we provide services within Young Offender Institutions or other settings involving children, we may process personal data relating to children. This is done in accordance with safeguarding legislation, UK GDPR, and relevant NHS and secure-estate requirements, with particular care taken to protect the rights and welfare of children.

4. How We Use Your Data

We process your data to:

Fulfil Contractual Obligations

Provide healthcare professionals (including GPs) to secure establishments under our contracts with NHS and private providers.

Manage Employment and Contract

Handle employment or self-employed contracts, timesheets, payroll, and pension obligations.

Legal Compliance

Ensure compliance with CQC requirements, NHS Trust protocols, and legal obligations such as safeguarding.

Communication

Keep you informed about work placements, updates to services, or other business-related communications.

Quality Assurance and Service Improvement

We use personal data to support clinical governance, audit, supervision, complaints handling and service improvement, ensuring that the care we provide meets best practice standards and contractual requirements.

Safety and Security

We process certain personal and compliance data to verify identity, manage access to secure environments, investigate incidents, and maintain the safety and security of the establishments in which we operate.

5. Legal Basis for Processing

We process your data under several lawful bases, including:

Performance of a Contract

To place you in employment or to provide healthcare services.

Legal Obligation

To comply with laws such as safeguarding, right to work, and tax legislation.

Legitimate Interests

To provide healthcare solutions to secure establishments, ensure the security of our business, and maintain relationships with NHS Trusts and private providers.

Special Category Data

When we process health information and other special category data, we do so under UK GDPR Article 9, including: Article 9(2)(h) – the provision of health or social care; Article 9(2)(b) – employment and social protection; Article 9(2)(g) – substantial public interest, including safeguarding and secure-estate requirements.

Data (Use and Access) Act 2025

Where we access or use NHS data, we comply with the Data (Use and Access) Act 2025, including requirements relating to secure data environments, data minimisation and transparency.

6. Sharing Your Information

We may share your personal information with:

Healthcare Facilities

The prisons, immigration centres, and other institutions where you are placed to provide medical services.

NHS Trusts and Private Healthcare Providers

As part of our contractual obligations.

Regulatory Bodies

The CQC and other regulatory organizations to ensure compliance with healthcare standards.

Third-Party Service Providers

To support operations such as payroll, background checks (e.g., DBS), or legal compliance.

All third-party service providers are bound by written contracts and are required to implement appropriate technical and organisational measures to protect your data, including compliance with NHS DSPT and, where applicable, Cyber Essentials.

Legal Authorities

Where required by law or to protect our business from fraud or other legal claims.

International Transfers

We do not routinely transfer your personal data outside the UK. If, in exceptional circumstances, such transfers are required, we will ensure appropriate safeguards are in place, such as adequacy regulations or the UK International Data Transfer Agreement (IDTA), and we will inform you where required.

7. Data Security

We implement robust physical, electronic and procedural safeguards to protect your personal information. These include role-based access controls, multi-factor authentication, encryption of data in transit and at rest, secure email solutions (such as NHSmail or equivalent), regular security testing and monitoring, and staff training in information governance and cyber security.

All data is stored securely on our systems, and access is restricted to authorised personnel only, based on job role and clinical or operational need. We maintain incident response and data breach procedures and will notify the Information Commissioner's Office and other relevant bodies where required by law. While we take all necessary precautions, the transmission of information via the internet is not completely secure, and we cannot guarantee the security of data during transmission.

8. Retention of Data

We will retain your personal information for as long as necessary to fulfil the purposes outlined in this policy, or as required by law. Typically, we retain employment data for 6 years after the end of a contract or placement, to comply with tax, NHS, and legal requirements.

We follow the NHS Records Management Code of Practice and relevant secure-estate and regulatory requirements when determining retention periods for clinical, safeguarding and incident-related records. Some records may be retained for longer periods where required by law or guidance.

More information regarding the retention of data can be found in the Records Management Policy Records Retention Schedule.

9. Your Rights

Under the UK GDPR, you have the following rights concerning your personal data:

Right to Access

Request access to the data we hold about you.

Right to Rectification

Request that we correct any inaccurate or incomplete information.

Right to Erasure

Request that we delete your personal data where applicable.

Right to Restrict Processing

Request a restriction on processing under certain conditions.

Right to Data Portability

Receive your personal data in a structured, commonly used, and machine-readable format.

Right to Object

Object to the processing of your data under certain circumstances, including for direct marketing.

To exercise any of these rights, please contact us at admin@drpasecure.co.uk.

We maintain a Record of Processing Activities and an Information Asset Register to support transparency and accountability. Where our processing is likely to result in a high risk to your rights and freedoms, we carry out Data Protection Impact Assessments (DPIAs) in accordance with UK GDPR and ICO guidance.

10. Cookies and Website Usage

We may collect technical information about your use of our website, including your IP address, browser type, and pages visited. This data is used to enhance the functionality of our website and improve user experience. Cookies may also be used for these purposes. For more details, please see our Cookie Policy.

11. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our business operations or legal obligations. Any significant changes will be posted on our website, and you will be notified where appropriate.

12. Contact Us

For any questions or concerns about this Privacy Policy or your data, please contact:
DRPA Secure

Email: admin@drpasecure.co.uk

Address: **42 Kew Court Richmond Road, Kingston Upon Thames, Surrey, KT2 5BF.**

For more information about your rights or to make a complaint, you can contact the UK Information Commissioner's Office at www.ico.org.uk or call **0303 123 1113** or Email: Casework@ico.org.uk (please ensure you include your contact number)

13. Jurisdiction

This Privacy Policy is governed by the laws of England. Any disputes arising out of this policy will be subject to the jurisdiction of the courts of England and Wales.

14. National Data Opt-Out

Where we process confidential patient information for purposes beyond direct care, we comply with the National Data Opt-Out policy. This means that, where applicable, your choice about how your confidential patient information is used for research and planning will be respected in line with NHS guidance.

You can find out more about the National Data Opt-Out by visiting <https://digital.nhs.uk/services/national-data-opt-out>