Privacy Policy

We, Clinical Response Group CIC, herein also referred to as CRG, respect your rights to data privacy and data protection when you communicate with us through our website, or other contact methods or when engaging with our staff as they complete their work.

If after reading this privacy policy you have a further privacy or data protection question, please contact us using the methods in the Contact Information section at the end of this document.

In this document we describe how CRG collects, uses, retains, and discloses personal information. Sometimes these policies might be referred to by others as a privacy policy, privacy statement, data policy, a fair processing notice or similar variations.

The Data Protection Act (DPA), the Human Rights Act (HRA), relevant health service legislation, and the common law duty of confidentiality pertain to what rights you have to control how we use your information.

CRG is a 'Data Processor' and depending on the data a 'Data Controller' for the purposes of the Data Protection Act.

CRG recognises the importance of protecting all personal and confidential information in all that we do and takes care to meet its legal & moral obligations.

To ensure that we process your personal data fairly and lawfully we are required to inform you:
- What types of data we may use;
- Why we need your data;
- How it will be used;
- Where it will be stored;
- With whom and under what circumstances it may be shared.

We only collect and use your information for the lawful purposes of administering the business of CRG and providing best practice of client care.

What Types of Information do CRG collect and why?
The types of personal information we use depending on the circumstances of our interaction with you might include:
- Personal details such as names, addresses, telephone numbers: so that we can communicate with you at your request such as for providing a service, training or CPD that you require or updating you on a status you have requested or necessity or for employment records;
- Family details for example next of kin details: for emergency or wellbeing notification purposes;
- Education, training & employment records of our staff: to ensure best practice in the services we provide;
- Financial details: where we provide a service for payment;
- Lifestyle and social circumstances; this may be needed to ensure safeguarding or the most appropriate treatment in accordance with a patients wishes;
- Visual images, personal appearance, and behaviour, for example if CCTV images are used as part of building security; this may be for the safety of staff and the public or property
- Details held in the patient's record: may be required for the safe planning and transportation of our service users;

• Responses to surveys, or other volunteered information such as where individuals have given feedback in relation to their interaction with us or other matters, including testimonials or reviews such as via email, letter, social media etc.

We may also process sensitive classes of information that may include:

• Racial and ethnic origin; may be relevant to best practice for patient care;

• Offences (including alleged offences), criminal proceedings, outcomes, and sentences: may be relevant for safeguarding or wellbeing of patients, staff, or the public;

• Trade union membership: ensure appropriate consideration given to employee representation;

• Religious or similar beliefs; helps to ensure appropriate interactions and care in accordance with the client's beliefs;

• Employment tribunal applications, complaints, accidents, and incident details; enables learning from past issues and establish best practice for non-re-occurrence;

• Clinical information such as infection status, allergies, diagnoses of medical conditions; may be relevant to well-being, diagnosis, or treatment;

• Medications prescribed and currently being administered; to assist with diagnosis or treatment;

• Physical data such as height and weight; may aid in assessing lifting and handling requirements or for relevant clinicians to assess medication dosage;

• Mobility or service users and details of any special instructions or equipment required; to ensure best practice in care;

• Physical or mental health details including any behavioural issues or triggers; to ensure best practice in care;

How will CRG use information about you?

In addition to the examples in the section above, your information is used to run and improve CRG. It may be used to:

• Check and report on how effective CRG is;

• Ensure that money is used properly for services it is commissioned to provide;

• Investigate complaints, legal claims, or important incidents;

• Make sure that CRG gives value for money;

• Make sure services are planned to meet patients' needs in the future;

• Review the care given to make sure it is of the highest possible standard;

• To improve the efficiency of healthcare services, by sharing information with NHS and sometime other organisations for a specific, justified purpose and approved by CRG.

We may keep your information in written form or on a computer. Whenever possible all information that identifies you will be removed.

How do CRG Store and Protect your Information

CRG only stores Personal Identifiable Information (PII) within the United Kingdom. Physical records are stored in CRG's premises which all have security monitoring systems in place. Physical records obtained off site are kept in a locked vehicle or in attendance of staff until such time that they can be taken to secure storage at CRG premises. Digital records are secured and encrypted, for protection on CRG's designated servers and transport via, to and from devices uses encrypted methods and trusted providers. We do not share our physical storage facilities with other organisations. This service is managed and monitored by CRG.

How does CRG Share your Information

There are many reasons why we share information. This can be due to:

• Our obligations to comply with current legislation;

• In the best interest of a vulnerable person; We must share information if the risk to the wellbeing of others outweighs the privacy concerns of the person to whom the data relates

• Our duty to comply with a Court Order;

- You have consented to or asked us for the disclosure of information.

We do not share your data with bodies outside of the United Kingdom.
We are aware of the requirements to ensure your data is protected against accidental loss or disclosure, destruction, and abuse. We have implemented processes to guard against such issues.

How Long Does CRG Retain Information?
CRG will only retain information for as long as necessary and whereby there is a legitimate and lawful interest in doing so. Records are maintained in line with our internal retention schedule which determines the length of time records should be kept. CRG record retention is kept to a minimum but will be dictated by legal requirements, insurance requirements and wellbeing requirements. Examples include if a potential crime has been committed info may need to be retained for future investigation. Info may need to be retained to disprove / defend against allegations such as in accordance with the limitations act or for reputational or insurance purposes.

CRG systems are updated on a rolling basis and security assessments performed to attempt to ensure best practices for the security of your data and the applications we use. Software, protocols, and hardware is reviewed and updated based on information from trustworthy relevant sources.

Third Party Sites, Communications and Services
CRG use Netlify & Unlimited Web Hosting for their website. As such they may log your IP address for reasons such as security purposes or other purposes in accordance with their privacy policy here…
https://www.netlify.com/privacy/
https://www.unlimitedwebhosting.co.uk/terms/privacy-policy
Our pages use scripts provided by jsdelivr whose privacy policy can be obtained here…
https://www.jsdelivr.com/terms/privacy-policy
Some pages use the Cloudflare Content Delivery Network whose privacy policy can be found here…
https://www.cloudflare.com/ru-ru/privacypolicy/
Our Get Quote link uses Jotform whose privacy policy is here…
https://www.jotform.com/privacy/
Our Contact Us page includes a map which is provided by google whose privacy policy is here..
https://policies.google.com/privacy?hl=en
Other links on the page such as via social media are subject to the policies of those provider which users would have agreed to in signing up for those services.

Some other parties may store logs such as phone numbers for billing by a telecommunications company etc.

Email: CRG uses servers maintained by Street Presence in the UK running regularly updated open-source software. Email uses TLS Transport Layer Security with Elliptic Curve encryption keys, SPF Sender Policy Framework to guard against spoofing and can use DKIM Domain Keys Identified Mail if required although Zen outgoing mail servers based in the UK may be used without DKIM. Staff of Street Presence, depending on authorisation, may log in via SSH Secure Shell from any location worldwide but the data is maintained in the UK. Street Presence only accesses any CRG data in accordance with CRG privacy policy and with CRG consent with the added security reasons where abusers' data, such as IP addresses, may be used to defend people and systems. Street Presence reports comment spam and illegal or abusive email activities to relevant authorities, web hosts, email providers and blacklists.

Cloud Services*:* CRG uses cloud services provided by Street Presence in the UK running regularly

updated open-source software. Forced secure access using Elliptic Curve encryption is enabled. Staff of Street Presence, depending on authorisation, may log in via SSH Secure Shell from any location worldwide but the data is maintained in the UK. Street Presence only accesses any CRG data in accordance with CRG privacy policy and with CRG consent with the added security reasons mentioned above. There are no third-party analytics used on the cloud system.
VOIP: CRG uses Soho66 based in the UK as a provider for VOIP phone operation so calls on our number can be put through to a relevant person where available. The system also accepts SMS, voicemail and faxes which are sent on as emails.
Data Storage: As updates are performed and improvements made, CRG evaluates the most appropriate means to process and store data available to them. This currently includes portable advanced encrypted storage volumes designed to avoid water marking attacks.

Cookie Policy
A cookie consists of information sent by a web server to a web browser and stored by the browser. The information is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.
We use “session” cookies on the website. We will use the session cookies to maintain a logged in user’s session and for order processing.
Session cookies will be deleted from your computer when you close your browser.
Most browsers allow you to reject all cookies, whilst some browsers allow you to reject just third-party cookies. For example, in Internet Explorer you can refuse all cookies by clicking “Tools”, “Internet Options”, “Privacy”, and selecting “Block all cookies” using the sliding selector. Blocking all cookies will, however, have a negative impact upon the usability of many websites, including this one.

Protecting your information
We take our duty to protect your personal information and confidentiality seriously. We are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.
We have appointed a Data Protection Officer/Data Controller who is responsible for the management of patient information and patient confidentiality.
All staff are required to undertake annual information governance training.
Under the CRG Contractor Agreement, all of our staff are also required to protect your information and inform you of how your information will be used. This includes, in most circumstances, allowing you to decide if and how your information can be shared.
Everyone working on behalf of CRG is subject to the common law duty of confidentiality. Information provided in confidence will only be used for the purposes advised and consented to by the service user unless it is required or permitted by the law.

How we Control Data
CRG has policies, procedures, and work instructions, detailing how we provide strict controls on both Data Security and Information Governance. The specific sections of areas covered are:

- Record Retention Storage and Disposal;
- Audit;
- Remedial and Preventative Action;
- Risk Management;
- Information Governance;
- Information Services;
- Information Services Code of Conduct;
- Secure Transfer of Information;
- IT and Data Security

• Information Governance Policy Statement;

What Information CRG collects about you?
We only collect and use your information for the lawful purposes of administering the business of CRG. These purposes include:

• Planning and booking Event Medical Cover and the continuation of care; such as booking us for medical cover or to continue an episode of patient care.

• Accounting and Auditing; in regard to submitting and receiving invoices and ensuring our clinicians are providing a high standard of care based on audits of their completed Patient Care Records.

• Accounts and records;

• Advertising, marketing & public relations; such as testimonials on our website or reviews via our Facebook or other social media platforms.

• Crime prevention and prosecution of offenders; where a crime has been committed, we may need to collect information about you in order to assist with the authorities and any investigations.

• Education; such as training courses and CPD sessions whereby attendees register their interest or book onto a course.

• Health administration and services;

• Information and databank administration;

• Staff administration; Such as ensuring our staff are legally able to work in a clinical setting and retain the right to work in the UK.

• Safeguarding; for the purposes of preventing harm to people.

How will CRG use information about you?
Your information is used to run and improve CRG. It may be used to:

• Check and report on how effective CRG is;

• Ensure that money is used properly for services it is commissioned to provide;

• Investigate complaints, legal claims, or important incidents;

• Make sure that CRG gives value for money;

• Make sure services are planned to meet patients' needs in the future;

• Review the care given to make sure it is of the highest possible standard;

• To improve the efficiency of healthcare services, by sharing information with NHS and sometime other organisations for a specific, justified purpose and approved by CRG.

We may keep your information in written form or on a computer. Whenever possible all information that identifies you will be removed.

Your Rights
You have the following rights in relation to the personal data we hold on you:

• The right to be informed about the data we hold on you and what we do with it;

• The right of access to the data we hold on you. This is known as a Subject Access Request.

These should go to dataprotection@teamcrg.co.uk or you can use our postal address found below. You will need to provide us with adequate information (for example your full name, address, date of birth, NHS number, employee number, etc.) so that your identity can be verified and your information located. You will also need to inform us of the specifics of what information you are requesting to enable us to locate this in an efficient manner such as the manner of interaction with us that gives you reason to believe we may hold data on you.

Where a fee is applicable under the terms of the Data Protection Act and subsequent legislation, we will inform you in writing. In due course our disbursement scheme (which outlines these fees) will be available.

We will endeavour to comply with a request within one month. However, we may need to extend this time period if the request is complex, or we have received multiple requests from an individual. If this occurs, we will contact the applicant and explain the why the extension is necessary. In some

circumstances, where a lawful exemption applies, we may refuse a request. If this is the case we will inform you of the reason why, your rights to complain to the ICO or other regulatory body and of your ability to seek to enforce this request through the courts;

• The right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'; We want to make sure that your personal information is accurate and up to date. If you think any information is inaccurate or incorrect or if you have a change in circumstances, then please let us know via email or contact us by phone on 01502 797616 or by accessing our webpage at: teamcrg.co.uk

• The right to have data deleted in certain circumstances. This is also known as 'erasure';

• The right to restrict the processing of the data;

• The right to transfer the data we hold on you to another party. This is also known as 'portability';

• The right to object to the inclusion of any information;

• The right to regulate any automated decision-making and profiling of personal data.

In addition to the above rights, you also have the unrestricted right to withdraw consent, that you have previously provided, to our processing of your data at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.
If you wish to exercise any of the rights explained above, please contact the Data Protection Officer at CRG.
Please email dataprotection@teamcrg.co.uk or write to us at Clinical Response Group CIC, 48 High Street, Lowestoft, Suffolk, NR32 1HZ.

Processing of Special Categories of Personal Data
The DPA provides some special considerations for certain types of data. CRG reserves the right to use these special provisions, especially Schedule 1, which states an exemption to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
Schedule 1: Processing is necessary for the purpose or preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnoses, the provision of health or social care or treatment or the management of health and social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Schedule 1.

Contact Information:

If you have a question about this Privacy Policy or how we use your personal information, please email dataprotection@teamcrg.co.uk or write to us at Clinical Response Group CIC, 48 High Street, Lowestoft, Suffolk, NR32 1HZ.

Complaints About how we Process Your Personal Information
In the first instance, you should contact the Data Protection Officer by Email: dataprotection@teamcrg.co.uk or by phone on 01502 797616 or by accessing our webpage at: teamcrg.co.uk
CRG is contactable 365 days a year between the hours of 8am to 6pm via telephone or 365 days a year, 24 hours a day via email (Preferred)
You can also email CRG at dataprotection@teamcrg.co.uk or enquiries@teamcrg.co.uk