Expert Cura LTD
71-75 Shelton Street, London, WC2H 9JQ
Email: contact@expertcura.co.uk
Web: www.expertcura.co.uk
Phone : 02039165072

Privacy Policy for Service Users

INTRODUCTION

Welcome to Expert Cura! At Expert Cura, we treat the privacy of our service users' personal data seriously. This policy identifies for you some key information about data processing and sets out the type of data we collect from you, why we collect it, and how we manage it. Managing data includes identifying the lawful basis for processing data, as well as how we gather, store, process, share, protect, and ultimately destroy data.

Our responsibilities relating to data processing are set out in the UK's Data Protection Act ("DPA") and the EU's General Data Protection Regulation ("GDPR").

In line with these provisions, data processing is overseen by our Data Protection Manager (DPM) whose principal duties are to inform, advise, and monitor our compliance with the DPA/GDPR.

Our DPM can be reached at contact@expertcura.co.uk or per mail using the above address.

WHAT IS PERSONAL AND SENSITIVE DATA?

Personal data means any information that may be used to identify you on its own or, when combined with other information, will enable identification.

Sensitive data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life and sexual orientation. In order to lawfully process this data, it is necessary to expressly consent to the processing.

We may collect, use, store, and transfer different kinds of personal and sensitive data about you, which we have grouped together as follows:

- *Identity Data*

  Identity Data includes first name, last name, username or similar identifier, date of birth, gender, and NHS number.

- *Contact Data*

  Contact Data includes your address, phone number and email address.

- *Health Data*

  Health Data includes any information about your physical or mental health from how you use our Services.

- *Usage Data*

  Usage Data includes information about how you use our services.

WHY DO WE COLLECT YOUR DATA?

Your personal data is required to effectively provide you with our services. In addition, key data may be used to support our safeguarding responsibilities and other statutory obligations. We also require

your data to measure the effectiveness of the services we provide and how they can be improved. This uses aggregated statistics, which do not identify you.

HOW DO WE OBTAIN YOUR DATA?

We use different methods to collect data from and about you including through:

- *Direct interactions*

  You may give us any of the categories of data identified above by filling out forms or by corresponding with us by phone, email, or otherwise.

- *Third Parties*

  We may receive your personal data from third parties who are referring you to our services. This is typically performed with your explicit consent but could be because there is a legal obligation that applies to the third party.

WHAT DO WE DO WITH YOUR DATA?

All of the data gathered is processed to effectively assess you for our services and provide you with a service accordingly. Our lawful reasons for processing data are detailed below, along with the type of data. Please note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

To register you as a new service user, we process your Identity Data and Contact Data. This is necessary for our legitimate interest to provide our services to you

To process and deliver a request for our services, we process your Identity Data, Contact Data and Health Data. This is necessary to provide our services to you, in other words, the fulfilment of our contract with you, and in relation to Health data, your express consent.

To manage our relationship with you, we process your Identity Data and Contact Data. This is necessary because we want to fulfil our contract with you and because we have other legal obligations, such as to keep our records updated and to study how service users use our services.

To comply with information sharing agreements, which can be for the purpose of Adult Safeguarding we process your Identity Data, Contact Data and Usage Data. This is necessary in order to protect your vital interests.

We will not use the personal data for marketing purposes. We will only use your contact details to correspond with you about the services we provide you with.

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us. If we need to use your personal data for an unrelated purpose, we will notify you, and we will explain the legal basis which allows us to do so.

RECORD KEEPING

We keep files on all our service users but only keep relevant information to ensure that the service we offer as an organisation is of the highest quality. The files are only available to staff who need to use them.

We make sure that:

- records required for the protection of service users and for the effective and efficient running of the service are maintained, are up to date and are accurate;
- service users have access to records and information about them held by the service, as well as opportunities to help maintain their personal records; and
- individual records and care service records are kept in a secure fashion, are up to date and in good order, and are constructed, maintained, and used in line with the GDPR, DPA, and other statutory requirements.

We adhere fully to the current standards on record keeping as set by the Care Quality Commission (CQC).

We consider that access to information and security and privacy of data is an absolute right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

DATA STORAGE

We take the security of personal data seriously. Your personal data is stored in electronic and paper files. We have internal policies and controls in place to try to ensure that data is not lost, accidentally destroyed, misused, or disclosed and is not accessed except by our employees in the performance of their duties. This includes:-

- an Internet-facing firewall to prevent outside penetration of our network. Policies allow mail to be delivered into the mail server from a specific set of addresses (our external spam filter), but no other access is allowed. This firewall also maintains a list that prevents access to malicious sites on the WWW.
- Spam filtering. All our mail passes through a spam filter, which looks for unsolicited mail, malicious software, and dangerous links.
- Local firewalling. All our machines are individually protected by firewalls. This prevents problem software proliferating through the network and unauthorised access from one machine to another, e.g., only the IT department can remotely connect to a company laptop.
- Local anti-virus to prevent any malicious software getting through the firewall or spam filters or being brought in by other means. Every machine has anti-virus software installed, which is constantly updated via a server on the network. This software also maintains a web blacklist to prevent access to malicious sites.
- File access controls. Access to data on the servers is controlled based on need. Management authority is required before any changes of access are made.
- Encryption. Our emails are encrypted when the recipient supports encryption.
- Filing cabinets. Data kept in service users' files are stored in lockable cabinets and secured in a restricted office.
- IT Policy. This policy is to ensure that all information technology users within Expert Cura or our networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within our boundaries of authority.
- Social Media Policy. This policy is aimed to educate employees and minimise risks when using social media, which can impact us and our staff.

SHARING YOUR DATA

Data is shared within Expert Cura as part of our lawful basis to process and is only shared relevant to the processing requirement.

We will not share data with third parties unless there is a lawful /regulatory / legal / contractual requirement or where you have given clear consent.

We will aspire to share the minimum amount of data necessary for the purpose and restrict the use of data that directly or indirectly reveals your identify. This can include anonymising your data or producing aggregated statistics or demographic information.

Examples of where we share such information in line with the above include:

a) Safeguarding obligations
b) CQC obligations
c) Contractual reporting
d) Health and Social Care Datasets
e) A referral made on your behalf with your clear consent
f) A referral made for medical purposes, including to protect your vital interests.
g) With any purchaser of the business in order to allow transfer of data to the buyer

We do not transfer any of your personal data outside of the UK and the European Economic Area.

Examples of third parties include but are not restricted to Care Quality Commission (CQC), Local Authorities, Clinical Commissioning Groups (CCGs), Public Health England (PHE), NHS Digital, Housing Associations, Hospital units, etc.

RETAINING YOUR DATA

We retain service users information only for as long as is necessary to provide the service. We will usually delete all your personal data within 12 months of our service to you ending. This is set out in our Data Retention Policy and Procedure.

DATA SUBJECT RIGHTS

Your rights
You can exercise the following rights:

- *Right to information*
- *Right to rectification*
- *Right to object to processing*
- *Right to deletion*
- *Right to data portability*
- *Right to withdraw consent*
- *Right to complain to a supervisory authority*
- *Right not to be subject to a decision based solely on automated processing.*

Update your information and withdraw your consent
If you believe that the information we hold about you is inaccurate or that we are no longer entitled to use it and want to request its rectification, deletion, or object (including withdrawing of consents you have given us) to its processing, please do so in your account or by contacting us.

Access Request
In the event that you wish to make a Data Subject Access Request, you may inform us in writing of the same. We will respond to requests regarding access and correction as soon as reasonably possible. Should we not be able to respond to your request within 30 days, we will tell you why and when we will be able to respond to your request. If we are unable to provide you with any Personal Data or to make a correction requested by you, we will tell you of the reasons why we are unable to do so (except where we are not required to do so by law).

What we do not do

- We do not request Personal Data from minors and children;
- We do not process special category data without obtaining prior specific consent;

- We do not use automated decision-making, including profiling; and
- We do not sell your Personal Data.

HELP AND COMPLAINTS
If you have any questions about this policy or about data protection at Bro Breakup in general, you can reach us at contact@expertcura.co.uk.

CHANGES
The first version of this policy was issued on January, 2025, and is the current version.