

Privacy Policy



Privacy Policy

It is simple – information that is about you is private.

European-wide laws which have been adopted in England via the Data Protection Act (2018) and associated legislation, sometimes referred to as the GDPR, (together the “Data Protection Legislation”) make it clear that the privacy of the person, to whom the information belongs, comes first. This means that the ways in which people and companies handle and store client’s personal information should be clearly explained, giving them increased control over data that is personal to them. There are some legal exceptions to this.

In this policy, we set out the different types of data, how data is handled and why, who handles that data, your control over your data and when we no longer hold your data.

ProblemShared is the trading name of Teledoctor Ltd (the “Company”) registered in England, (company number 10410380) at 3 Frederick Street, London WC1X 0ND. The Company provides access to mental health care services via its digital platform problemshared.net (the “Platform”). This encompasses a network of mental health practitioners (each a “Practitioner”) who provide their services remotely via video link to users of the Platform.

This Privacy Policy which is available on our Platform also forms part of our User Terms and Conditions, consent to which we ask you at the point of signing up and booking a session with one of our mental health Practitioners.

If for any reason you wish to contact us regarding privacy and your personal data, please contact our Data Compliance Officer careofhelp@problemshared.net

(Capitalised terms in this document have the same meaning as in the User Terms and Conditions, unless specified otherwise.)



<u>Index</u>	<u>Page</u>
1. <u>What Information</u>	<u>4</u>
a/ Different types of information	4
b/ Information we ask you to provide	4
c/ Information you may choose to provide	5
d/ Information that is collected by us	5
2. <u>Why & How Information is Used</u>	<u>6</u>
a/ What does this mean?	6
b/ Our prime purpose	6
c/ Ancillary but still part of our purpose	6
d/ How do we do that?	7
3. <u>Control of your information and Consent</u>	<u>7</u>
a/ Cookies	7
b/ Privacy Controls	7
c/ Key information	7
d/ Disclosure	7
4. <u>Privacy and Mental Health Practitioners</u>	<u>7</u>
5. <u>Who Uses It</u>	<u>8</u>
a/ Data controller	8
b/ Partner Organisations and Subsidised Sessions	8
c/ Sharing with 3 rd party data processors	8
d/ Other types of access	9
6. <u>Security</u>	<u>9</u>
a/ Authentication	9
b/ Data Transfer	9
c/ Storage	9
d/ More information	9
e/ Your responsibility	9
f/ No guarantee	9
7. <u>Your access to and rights over your personal data</u>	<u>10</u>
a/ Information you can access	10
b/ Digital Records	10
c/ Your rights of access etc	10
8. <u>Complaints</u>	<u>11</u>
9. <u>When we no longer hold your data</u>	<u>11</u>



1. What information?

a/ Different types of information

Personal information is defined as that which, whether on its own or in combination with other information, allows for the identification of an individual. Information that relates to a person's health is also sensitive information. Where personal identifiers are removed from the information, and the information is anonymised and then aggregated, this is no longer personal information.

There are different contexts in which we hold information about you. These are associated with discrete, albeit related, purposes, and are also associated with different mechanisms for control by you. We first set out each of the different contexts for information, next we describe our purposes, and then we address control over data, the relationship with mental health practitioners, processing of data and your access and rights over data, complaints and when we no longer hold your data.

b/ Information we ask you to provide

We ask you for certain information in connection with your use of the App and any sessions you book with a practitioner.

This includes:

i/ your full name, email address and mobile telephone number which we use to identify you, to create a Booking, and to contact you in relation to your use of the Platform and in relation to the therapy you receive over the Platform, and this information is stored in your Profile;

ii/ your date of birth, your GP's name and GP practice contact details to further identify you and your primary health carer, as part of your intake form ahead of your first appointment with a Practitioner. Information collected from your intake form is not stored in your Profile;

iii/ an emergency contact in case of emergency as part of your same intake form;

ii/ information connected with why you wish to see a Practitioner, or your medical history which you may choose to provide in as much or as little detail as you like, again as part of your intake form. This information is sensitive information, and is not stored in your Profile;

iii/ billing or payment information you provide in connection with a booking but which we do not store and which is handled by our third party supplier;

v/ any feedback from you in the event that you participate in a survey of the Platform.

You will be guided and prompted in filling in any required information fields on our intake form over the Platform.



You can review and update your Profile in the App at any time, and you are obliged to update these details in case of change.

You are solely responsible for the truth, currency, accuracy and completeness of the information that you provide to us.

c/ Other Information that you may choose to share with your Practitioner or with us

We do not store information that either you or the Practitioner choose to share with each other during the course of your session via separate email, for example a document with suggested exercises as part of your therapeutic relationship. In the event that you and the Practitioner share a document or file by email that contains information that is personal to you, the Practitioner is the person who controls and stores that information for the purposes of privacy. In the same way, the Practitioner may make notes of their Session with you, and this information is also personal to you. We address this later in the policy since Practitioners also hold, control, handle or process your information in this regard.

The content of any communication between you and us, separate to your Practitioner, also contains information relevant to you. When you contact the Company by email or telephone for whatever reason, we will keep a copy of that email or a note of that conversation.

d/ Information that is collected by us

Each time you visit the Platform, we collect the following information about your digital activity including but not limited to the following:

i/ device specific information: the type of device (mobile or tablet) you are using; temporary or persistent unique device identifiers (UDIDs), the I.P. address of your Device, your mobile operating system, the type of mobile internet browsers you use;

ii/ usage information: the full uniform resource locator (URL) clickstream to, through and from the Site (including date and time); menu items, or pages you viewed or searched for; page response times; download errors; length of visits to certain pages; page interaction information (such as scrolling, clicks and mouse-overs); actual duration of video-link consultation during any Session in minutes; recurrence of visits to the Platform; recurrence of Sessions that you book; methods used to browse away from one page of the Platform and another, and any phone number used to call us at ProblemShared.

2. Why & How information is used:

The Company will use your information only as is legally permitted. We may interact with your data in a number of ways or contexts: we receive or request data from you, we receive or request your consent or change of consent with respect to your data, we store data, we handle and use it, we direct or permit others to handle or use it, we provide copies of it to you at your request, and we eventually delete it.

a/The extent of our access - Legally we must have good reason to use your data, and we must keep it private, and where that data does not remain private, it must only be where we



are required or permitted by law to disclose it. In handling data, it is important to note that when the data has been anonymised it is no longer personally identifiable.

b/ Our prime purpose in handling your personal information is to facilitate your mental health care, and to give effect to the contract you enter with us for your use of the Platform and to give effect to the contract you make with the Practitioner that is seeing you. We provide a centralised platform over which Practitioners can serve the mental healthcare needs of clients such as you in a remote setting via video-link consultation.

How do we do this? This includes verifying you are a real person, and that you are who you say you are; enabling payment for Sessions; facilitating a Practitioner's understanding of your history, including, if relevant, a Psychiatrist's understanding of your medical history; your reasons for seeking treatment; previous medications etc; contacting you if needed; managing any complaint you make, and otherwise communicating with you in relation to your use of the Platform, eg via email, and sending you automated reminders about your Bookings.

We may also use your contact details to send information about updates and features of the Platform on an ongoing basis. We will only do this where you have opted in to receiving such marketing. We do not provide data for third parties to market to you.

c/ Ancillary but still part of our purpose of providing a remote mental health care service via our Platform is the improvement and further development of the Platform itself, for the mutual benefit of the Company, Practitioners and Clients such as you to deliver a mental healthcare service that is user-friendly, secure, helpful, informed and responsive.

d/ How do we do that?

We also use information about how and why the Platform is accessed for our own analysis of efficiencies and operations of the Platform.

So we may also use data that is collected regarding devices and usage of our Platform for various technical reasons, such as troubleshooting, improving operations, and efficiency, statistical analysis, research, and survey purposes for Platform and service optimisation, and to monitor security of the Platform and protect against inappropriate or unpermitted use of the Platform as per our User Terms. Cookies and similar technologies may be used to collect this information.

On a broader level, we may also use data that informs about patterns and presentation of mental health matters to better inform our approach to providing tailored and representative services, and to contribute to broader dialogue in communities associated with mental health care.

In both contexts of specific application to the Platform and to the broader context of the mental health space within the community, this analysis is done via combining and aggregating amounts of data that are first anonymised, which means that, at that point, the data no longer constitutes personally identifiable information and it is mixed with lots of other information.



We may share the results or conclusions of our analysis with you and other users over the Platform in the resources we make available via the Platform, or we may share with our network of Practitioners, and third party suppliers to better educate others of information relevant to mental health care and treatment, and to delivery of services over the Platform. Such information would be based on analysing anonymised aggregated data as set out above.

3. Control of your information & consent:

a/ Cookies - You may refuse the use of cookies and other such features that help us understand user's interaction with the Platform by making your selection when you access the Platform. See our Cookies Policy.

b/ Privacy controls - You may also request that we do certain things with regard to information about you as per section 7 – Access and rights.

c/ Key information - Without certain information of yours, that goes to identify you, we cannot grant you access to the Platform since we cannot create a profile for you nor facilitate Bookings with Practitioners. Nor can we provide access to therapy with your choice of Practitioner without sharing personal and sensitive information about you with your chosen Practitioner such as that contained in your intake form.

d/ Disclosure - We must also obtain your consent first before we disclose any personally identifiable information to any other third party, for example your GP.

If we disclose personally identifiable information about you without your consent, then we can only do so where our action is necessary by way of a legal claim, or as required by any enforcement or other government agency, or as is necessary under any competing law or regulation, for example a public health interest, or in case of emergency or for the purpose of safeguarding against harm to You or another person; to investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of our services.

4. Privacy and Practitioners:

The Practitioner you see in your session is also bound to follow and comply with all relevant laws about privacy, like us. And the agreement you make with them in defining your therapeutic relationship should also address your rights and the Practitioner's obligations about privacy in connection with the information that they handle, hold and store about you, including the information that is stored on the Platform to which your treating Practitioner has access (your identification and contact information and the sensitive information that is contained in your intake form), and information that is part of the records they create of their sessions with you, such as a Practitioner's Notes.

Practitioners are not only bound by strict confidentiality as per their relevant professional body's code of ethics, and by contractual agreement with the Company, they can also only



use your data in the ways specified by the relevant laws such as the Data Protection Legislation.

Practitioners are bound therefore to address with you matters akin to those we address here – what information is held, how it is handled or shared, and your rights to access it and your consent to its use.

With regard to recordings of any session, we note that there is no opportunity for any recording to be made over the Platform. Should there be any request to record a session with a Practitioner, this must be evidenced in writing as agreed between you and the Practitioner as proof of your consent, alongwith provisions for the purpose and format of such recording, use, processing, handling and storage and deletion, as would be usual for privacy law requirements.

5. Who uses it:

a/ Data controller – For the purposes of the Data Protection Legislation, the Company (Teledoctor Ltd) is a registered controller of information it holds about you and it has a Data Registration Number with the UK supervisory body - the Information Commissioner’s Office.

As noted above, a Practitioner also has access to, stores and handles information about you. That Practitioner must also be registered with the ICO for the same purposes as us.

b/ Partner Organisations and Subsidised Sessions - Where your session is part of an arrangement with a tertiary institution or other organisation (“Partner Organisation”), under a subsidised cost arrangement, we will not share any information with the Partner Organisation except information without which we are unable to facilitate the sessions, nor arrange payment or settlement of such subsidised costs of the sessions.

c/ Sharing with Third Party Data Processors - The Company uses other companies to provide data processing services on our behalf, for a range of purposes including facilitating the integration of parts of the Platform, facilitating payment for Sessions, optimising functions of the Platform, analysing access to and engagement with the Platform.

With regard to personally identifiable information that enables payment for services, we do not store any such information. The third parties who are our suppliers of billing and payment function systems, credit checking or encrypted security solutions must be compliant with Level 1 Payment Card Industry (PCI) data security standards. Any payment transactions are encrypted using SSL technology.

Your information may be processed in such a way that it is made anonymous so that you cannot be personally identified (for example, name deleted and gender, age, address details unlinked so that no person can be identified), and is then aggregated with other data to allow analysis.

Where we do share information with third party data processors, this will not be processed or stored via destinations outside the European Economic Area. In the event this changes, it



shall always be processed or stored in accordance with applicable data protection laws in England and subject to strict safeguards.

d/ Other types of access - As noted earlier, the Company may be required to provide information to others in the context of legal, enforcement or other governmental obligations.

6. Security:

The Company takes appropriate technical and organisational measures to guard against unauthorised or unlawful processing of your personal data and against accidental loss or destruction of, or damage to, your personal data as required by the Data Protection Legislation. The Company has security measures in place and it engages third party to supply to us systems that integrate with the Platform, which companies are also bound by the Data Protection Legislation in their contracts with us.

Some of these measures include:

a/ Authentication – confirmation of username and password and as may be required or adopted: 2 factor authentication.

b/ Data Transfer – Data in transfer is fully encrypted using the most secure cryptographic technologies available (256-bit level of encryption).

By encrypting electronically transmitted information such as video calls or messages, this information can only be accessed by the participating parties. With encryption, the rest of the information is distorted and unreadable, impossible to interpret without special keys.

c/ Storage – All information is stored on secure servers which have achieved the highest level of security certification and are located in UK-based data centres.

d/ More information - Our third party suppliers or processors are also bound by the Data Protection Legislation in their contracts with us. If you require any more information about the security measures we take in carrying out our obligations under the Data Protection Legislation, please contact our Data Compliance Officer care of help@problemshared.net

e/ Your responsibility - It remains your responsibility to ensure no-one else uses the Platform in your place, or gains access without your permission, and you are responsible for keeping your access private.

f/ No guarantee - Of course, no data transmission over the internet can be guaranteed to be 100% secure. While the Company undertakes to the best of its ability to protect your personal data from unauthorised access, use or disclosure, the Company cannot ensure or warrant the security of any information you transmit via the Platform, including during your session.



7. Access to and Rights over your Data

a/ Information you can access without contacting us - The Company makes access to your personal data immediately available in the following ways:

i/ You can access the information that we hold about you for Booking purposes by logging in to the Platform.

ii/ You may request that the Practitioner attending your Session send to you by email a copy of any Referral letter if s/he has sought a referral on your behalf.

b/ Access to Digital Records: The Company only permits the Practitioner/s responsible for Session/s with you to update or add to your Digital Record; your Digital Record is inaccessible to others apart from any person authorised by CQC guidelines for medical purposes such as the clinical lead to ensuring best practice and compliance with CQC requirements.

c/ Your Rights of access, correction, erasure, restriction and consent withdrawal – Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, request the restriction of processing or request that we transfer a copy of your personal information to another party, please email our Data Compliance Officer care of: help@problemshared.net

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly



unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please email our Data Compliance Officer care of help@problemshared.net

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

8. Complaints

You may contact us regarding any complaint at help@problemshared.net

Alongside your right to contact us to make a complaint or other request with regards to your privacy, you may also contact the Information Commissioners Office (the data protection regulator in the UK): Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, telephone: 0303 123 1113 (local rate).

9. When we no longer hold your data

We hold information personal to you for a period of seven (7) years after the therapeutic relationship ends with a practitioner.

With regard to medical records pertaining to psychiatric-based treatment over the Platform, we hold that part of your record in accordance with national best practice guidance as issued by the British Medical Association, Department of Health, and/or relevant NHS codes. But of course, we may retain personal data for other periods as required by any other law or regulation.

Type of record	Retention period
Records relating to persons receiving treatment for a mental disorder within the meaning of mental health legislation	20 years after the date of the last contact; or 10 years after the patient's death if sooner.

