

Guidance for COSRT Members on Preparing a Privacy Statement

COSRT.ORG.UK INFO@COSRT.ORG.UK TWITTER: @COSRTNEWS



CONTENTS

Introduction.....2

What you should include:.....2

Why are you are collecting the data, e.g. what are you going to use it for?3

Are you going to share the data how and why?3

Case studies and taping sessions.....3

Supervision4

Trainers.....4

How will you store any data4

How long will you store any data4

How can clients access the data and can they ask to be “forgotten”?.....4

Data Breaches.....5

Person responsible for Data Protection5

Use of Cookies and Analytics.....5

Please note5

Introduction

On 25th May 2018, the EU General Data Protection Regulation (GDPR) replaced the UK's Data Protection Act 1998 (DPA), becoming the Data Protection Act 2018. This will apply even after the UK leaves the EU.

Since the DPA was passed a lot has changed in the world of data protection. New technology and social networks make it easier than ever to access, use and share data. It is therefore very important to make sure data protection laws are fit for these developments in communication. The GDPR brings everyone up to date, by strengthening and unifying data protection for all individuals within the European Union (EU).

We recognise your concerns about the GDPR and what it means for your day-to-day clinical practice. While there will be some changes to the way we all handle personal data, the GDPR builds on the foundations which you already have in place. Sometimes there are no specific answers and many of the decisions regarding data need to be made individually with due consideration to your personal practice. The information given below may help you write your privacy statement, but it is a guideline only and not exhaustive. This statement needs to go on your website if you have one. Extracts may also be included in the documentation you give to your clients.

What you should include:

Controllers name

This is your practice/business name. You will need to register with the Information Commissioner's Office, and you can include your registration number. The ICO register will hold the address on the public register, but this can be a registered office address, rather than home address. Many accountants and solicitors offer a registered address service.

What personal data are you asking for?

You may be asking for the following information. Information may be personal or sensitive.

The personal information:

- Name
- Address
- Email Address
- Landline Number
- Mobile Number
- Date of Birth

- Qualifications
- Financial information, including bank account details.

Sensitive personal information, or special category data includes:

- Gender, ethnicity, and marital status
- Religious or other cultural beliefs
- Physical or mental health or condition
- Sexuality
- Offences (including alleged offences)

Why are you collecting the data, e.g., what are you going to use it for?

Think carefully why you are collecting, and how you are using, the data and describe this in simple, clear language that the client can understand.

Are you going to share the data how and why?

Who do you share data with? This may differ from client to client and may need personalising. For some of your clients it maybe no one. Whereas for other clients, it may be other individuals e.g., GP, social workers, probation services etc., or even a team. You may need to obtain explicit consent in this case. You must be clear and be willing to personalise. You must be able to justify why you are legitimately sharing data, for example any sharing of information with payment platforms, and be explicit about this. On occasion you may be required to share information with government agencies, e.g., for safeguarding or criminal matters – you should make this clear.

You also need to think about issues such as client safety and safeguarding when you may share information without consent. Also, the need for additional security and additional consents and procedures for safeguarding if you are dealing with children. Children may give consent to the use of their personal data from the age of 13.

Case studies and taping sessions.

Many training organisations require the use of case studies and taping as an integral part of their course. If client data is going to be used as part of a case study or taped presentation, this must be consented to separately and there must clear information as to how this information will be used and who will see/hear it. This should be additional to the client agreement and there must be a new agreement for each time the client is used as the subject of a case study or taping. All case studies and tapings must be anonymised. Training

institutions should have a clear protocol as to how this data sharing is managed within their system and you should ensure that this is adequate to protect your clients.

Supervision

Supervision is part of our professional duty of care to our clients. There must be clear information as to how a client is referred to in supervision sessions and how any notes are anonymised, stored and destroyed.

Trainers

Trainers on COSRT approved courses must be clear with trainees about their links to COSRT and that information about their trainees is shared for professional training purposes only. This must be explicitly stated in the privacy statement.

How will you store any data?

Be explicit as to how you protect your client's data by your method of storage and how it will be secured, for example password protected.

How long will you store any data?

This will generally be seven years. See more information under subject access.

Disposal – How will you dispose of the stored data?

Again, be explicit about how computer information and hard copies will be destroyed e.g., by shredding etc. If you are a trainer or trainee and have used taping or case studies as part of clinical work, you must obtain separate consent for this and have a clear protocol of how this will be shared, used, stored, destroyed, and anonymised throughout the entire process to protect the client.

How can clients access the data, and can they ask to be “forgotten”?

Should a client wish to access your data, or have it destroyed before 7 years have elapsed, they may submit a request in writing to you as the Data Controller. They are also entitled to amend their information. You must ensure that it is the subject requesting this information and not a third party. You must respond to their request within a month and not make a charge for providing any information. Where subjects are asking that their information be deleted, you will need to keep a suppression list to evidence that you have complied with their request.

Each application will need to be considered on an individual basis and any decision to provide access to or destroy personal data will be your clinical decision. Please note safeguarding will always be a priority over personal freedom. Information about third parties must never be disclosed without their express consent.

Data Breaches

There are particular challenges in features/programmes that involve 'real people'. Here are some Ethical Guidelines; if you feel they are being breached, you need to challenge that with the programme producers and if necessary, withdraw from the project.

Person responsible for Data Protection

You must name who this person is. In a one-person practice this will be the clinician. In a larger practice it could be an administrator.

Use of Cookies and Analytics

- Give details of how your site uses these.
- Use of cookies
- Use of website analytics - e.g., shows number of website visits etc.
- Google analytics
- Any plugs in you have etc.
- Links to third parties' sites

The privacy notice re cookies should be available on every page on the website in case a client only goes to your blog page, so it's normally in the page footer. This should link to the privacy policy also.

Please note.

Your privacy statement should be separate from your client agreement and show clear evidence of consent – who, when, how, and what you told people. It should be signed independently of the client agreement. It should allow for consent being withdrawn at any time.