Confidentiality and UK GDPR Guidance

March 2024

Contents

Overview

About us

The British Psychoanalytic Council (BPC) is a regulator set up to protect the public. We set and uphold the BPC code of ethics. We keep a register of professionals who are required to meet our standards for their professional training, knowledge, skills and behaviour. The people on our register are referred to as 'registrants'.

About this guidance on confidentiality

We have produced this guidance to help Registrants meet specific standards in relation to confidentiality. We keep supporting guidance under regular review.

[1] The term "therapist" also refers to psychotherapists, psychoanalysts and counsellors

This version – together with separately published Code of Ethics replaces any previous BPC guidance on confidentiality.

Patients[2] and the public

If you are a patient in treatment with one of our registrants, or a member of the public considering treatment with one of our registrants, the confidentiality guidance will help you understand how they should behave towards you. On the rare occasions that something goes wrong, anyone can raise a concern through our fitness to practise process. We can take action when there are serious concerns about a registrant's knowledge, skills or behaviour. We use the code of ethics to help us decide in each case whether we need to take action to protect the public. The current code of ethics can be found here

BPC registrants

If you are registered with us, you must make sure that you are familiar with the standards and that you continue to meet them which includes your responsibility towards confidentiality and GDPR. If you are applying to be registered with us you will need to complete a declaration once you are registered to confirm that you will keep to the standards.

As a registrant, you are personally responsible for the way you behave. You will need to use your judgement so that you make informed and reasonable decisions and meet the required standards at all times. You must always be prepared to explain or justify your decisions and actions.

Making informed and reasonable decisions might include getting advice and support from your Member Institution (MI), colleagues, education providers, professional bodies, or other people.

Introduction and Scope of Guidance

Following the coming into effect of the Data Protection Act 2018 ('DPA 2018') and the United Kingdom General Data Protection ("UK GDPR"), this Guidance is in two parts.

Part 1 of this document offers guidance regarding the **DPA 2018 and UK GDPR**, specifically regarding the **kinds of patient information** covered by DPA 2018 and UK GDPR and **registrants' responsibilities** regarding such patient information.

Part 2 of this document addresses the following questions:

[2] The term "patient" refers to both patients and clients

(1) What is the **relationship** between the **therapist's duty of confidentiality** and the **DPA 2018/UK GDPR** ?
(2) How do the **DPA 2018/UK GDPR affect** the long-standing and respected **tradition of sharing clinical knowledge and experience** generated in the course of the therapeutic endeavour in publications, conference presentations, lectures, qualifying papers and more generally for training purposes?
(3) What are the **particular ethical considerations regarding confidentiality** to be taken into account when writing or teaching involves **using clinical material where the patient is likely to recognise themselves or be recognised by others** ?

Part 1: the Data Protection Act (DPA 2018) and UK General Data Protection (UK GDPR)

The Data Protection Act 2018 ('DPA 2018') and the UK GDPR require therapists to be clear with their patients about what information relating to them they collect, how they use such information, the lawful basis on which they rely for such use, and their patients' rights regarding such use. Thus, the scope of therapists' professional duty of confidentiality needs to be considered against this statutory background. Registrants need clear guidance about their ethical **and legal** responsibilities regarding patient information, so that they can decide how they are going to discharge those responsibilities and so that they can be accountable for their decision making.

Categories of information

The DPA 2018 and the UK GDPR apply to the processing of "personal data", defined as "any information relating to an identified or identifiable [living] person", either by automated means or as part of a manual filing system. At least the following two broad categories of information typically held by registrants in private practice may fall within this definition:

Category 1: Patient's identity (name, address and other contact details); fact identified (or identifiable) patient is in therapy and duration of therapy; details of days, times, and frequency of their appointments.

Category 2: Provided that patient or third party is identifiable from any such details or combinations of such details: details of patient's personal history, family background, presenting problem, and present and past relationships with third parties; and occurrences happening over course of therapy (in patient's personal life, in personal lives of third parties known to patient, or in therapy itself).

Generally, if a registrant in private practice records any information of this kind, they need to take the following steps in accordance with the DPA 2018 and the UK GDPR:

(1) Conduct an **information audit** to determine exactly what information they process and who has access to it, securely destroying or anonymising all patient information they no longer need to keep;

(2) Assuming the outcome of the audit shows that the registrant holds or handles any information within either of the two categories noted above, **register** with the Information Commissioner's Office ('ICO') as a data controller;

(3) Demonstrate **transparency** by providing patients at the earliest possible opportunity with a **Notice** ('UK GDPR Notice")[3] which:

  (a) Provides the registrant's name and contact details;

  (b) Specifies the kinds of information held (e.g., patient contact details, post-session notes, payment records);

  (c) Specifies the purpose(s) for which such information is processed (typically necessarily in order to provide the patient with competent and ethical therapy treatment) and the lawful basis on which it is processed (typically consent and/or performance of a contract);

  (d) Identifies (without naming) with whom such information is normally shared (typically supervisor and clinical trustees);

  (e) Specifies the circumstances in which such information is exceptionally shared otherwise than in (d), including, but not limited to, the following well-recognised exceptions to the ethical duty of confidentiality:

    (i) if the registrant reasonably considers it necessary to preserve the patient's life or that of another person;

    (ii) if ordered to do so by a court of law;

[3] Registrants who enter into written contracts with their patients need to be careful to ensure consistency between the terms of that contract and the UK GDPR Notice they provide to their patients. If the written contract precedes in time in the UK GDPR Notice, registrants may wish to include in their UK GDPR Notice a statement that the Notice should be understood as an agreed modification of the parties' rights and obligations under their contract.

(iii) if the registrant has information which they know or believe might materially assist in the prevention of an act of terrorism or in securing the apprehension, prosecution or conviction of a person in the UK for an offence involving the commission, perpetration or instigation of an act of terrorism (s. 38B of Terrorism Act 2000);

(iv) if the registrant reasonably decides to comply with a request under Schedule 2, Part 1, paragraph 2(1) of the DPA 2018 (usually from the Police) to disclose information in order to prevent or detect crime, or apprehend or prosecute offenders; or

(v) if the registrant needs to recover unpaid fees;

(f) Specifies for how long the information is (justifiably) held;

(g) Advises the patient of their rights to complain to the ICO (about the registrant keeping or sharing their information), to see the information kept by the registrant, and (if inaccurate) to have it corrected, erased, isolated, and to object to the registrant continuing to keep it.

(4) Demonstrate **accountability**, typically by carrying out a Data Protection Impact Assessment which shows that appropriate safeguards are in place to protect the relevant information, having regard to its high-risk character (as so-called "special category data" under the UK GDPR), and by creating and maintaining a document which evidences systematically the registrant's compliance with data protection law and which logs data breaches (e.g. unauthorised disclosure or loss of patient information).

Key principles of UK GDPR

Transparency, lawfulness, accuracy and **accountability** are key principles of the UK GDPR. A further key principle is **security.** Registrants in private practice need to consider carefully the security of their arrangements for keeping safe the kinds of patient information categorised above (e.g. encryption or password-protection of information on computer including email content; storage of paper records and notes in a lockable filing cabinet; and use of pseudonymisation, such as code-numbers, to link contact details and other patient records). All these arrangements should be evidenced in the document referred to in (4) above. Further, data security breaches need to be reported to the ICO without undue delay (within 72 hours) unless the breach is unlikely to put their rights and freedoms, or those any other living person, at risk. Where the breach is likely to result in a **high** risk to any living person's rights and freedoms, it must also be reported to the affected data subject(s) without undue delay.

Still further key principles of the UK GDPR are **purpose limitation**, **data minimisation, storage limitation** and **fairness.** How much patient information is held and for how long ought to be related to the lawful purpose for which that information is used or held. Moreover, where a particular purpose has been identified and documented in a UK GDPR Notice, that information cannot be used or held for an incompatible purpose. Regarding **fairness,** patients should not be deceived or misled about registrants' use of their information and such use should be within their reasonable expectations. They should not be unjustifiably harmed by their therapists' use of their information.

Part 2: Therapists' Duty of Confidentiality and the DPA / UK GDPR

Therapists' ethical duty of confidentiality

Having regard to the DPA 2018/UK GDPR Guidance set out above, what is the relationship between the therapist's duty of confidentiality and the DPA 2018/UK GDPR: how might the therapist's ethical duty of confidentiality now be understood?

The therapist's ethical duty of confidentiality has a very specific foundation. That foundation is the trust and confidence which are intrinsic to the psychoanalytic undertaking. The ethical duty of confidentiality is both the corollary of the patient's expectation that they can express themselves freely and essential for containment. In short, confidentiality is necessary for the work. Further, the reality that in a clinical encounter the patient trusts and expects their therapist to keep their confidentiality in and of itself engages the ethical values of fidelity, respect and justice, requiring the therapist to honour the trust placed in them.

Although there is certainly overlap between the latter ethical values and certain of the key principles informing the UK GDPR (in particular, the operation of the key principle of fairness), the emphasis is different, with the focus by the UK GDPR on the specific privacy rights of the data subject and the responsibility of the data controller to respect those rights. The result is that the therapist's professional duty of confidentiality is neither reduced nor expanded by the GDPR, but rather that the UK GDPR has defined and codified patients' legal rights regarding information capable of identifying them in the hands of their therapists. Thus, registrants post-UK GDPR are subject to both the ethical duty of confidentiality **AND** the UK GDPR's

detailed network of specific tasks to be undertaken **by anyone** handling information capable of identifying a (living) person.

Notes on clinical material

How do the DPA 2018/UK GDPR affect the use of clinical material in publications, conference presentations, lectures, qualifying papers and more generally for training purposes?

Although the UK GDPR can be understood generally as separate and parallel to the ethical duty of confidentiality, there is one aspect of professional life where the interaction of the duty of confidentiality and the requirements of the UK GDPR requires particular attention. This concerns therapists' use of clinical material in publications (including broadcasts, podcasts and any other medium for dissemination of information to the public), conference presentations, lectures, qualifying papers and more generally for training purposes.

In recent decades, the ethics of using clinical material outside the consulting room have received closer scrutiny. This is a complex issue involving competing considerations of fairness with strongly argued perspectives of where the balance should be struck between protection of the patient's confidences and the interests of all patients in having well-trained therapists who share valuable clinical expertise and knowledge. For some, the inequality between therapist and patient and the influence of transference in the analytic situation make it questionable whether patient consent to use of clinical material can ever be regarded fairly as informed consent, that is to say, consent freely or autonomously given. Therefore, it is argued, the problematic nature of consent means that, even with consent, disguise is always necessary. However, even then, disguise cannot be relied upon as a cure since it is often ineffective or effective only at the expense of clinical truth. Even with consent and effective disguise, further ethical considerations arise regarding the therapist's ethical duty not to do harm and the intrusion of the request for consent into the analysis or therapy; the impact on the patient of such request depending upon its meaning for them in their internal world and with their particular personal history; and the further impact on them of later learning what their therapist has said or written about them and their analysis or therapy.

The UK GDPR does not assist the practitioner struggling with the difficult ethical questions surrounding whether or not to write (or teach) about their patient. It has, however, its own specific impact: if the practitioner decides to write (or teach)

about their patient and the information intended to be used (in the paper or lecture) is capable of identifying their patient, since such use cannot fairly be regarded as necessary for the provision of therapy to their patient, in order to comply with data protection legislation, in practical terms, if the therapist's UK GDPR Notice explicitly covers the use of patient information for the purpose of the therapy and the sharing of such information for that purpose only with supervisor and clinical trustees, its use for the new purpose (of publication or teaching) now needs the patient's explicit consent. Moreover, the relevant UK GDPR legislation requires that that consent must be explicit, freely-given, informed, affirmative (by statement or action) and unambiguous, with a genuine choice being offered, and that it is able to be withdrawn at any time.

Against this legal background, what becomes critical from the point of view of teachers and writers in the field is whether the relevant patient information can fairly be regarded as identifying, or capable of identifying, the patient, because it is only if this initial requirement is satisfied that the further requirement for specific consent arises. On this narrow issue, the following guidance is offered:

(a) Where clinical material is to be used and the use of anonymisation and disguise mean that no-one including the patient would be likely to recognise themselves, explicit consent is not required by the UK GDPR;
(b) Where clinical material is to be used but the use of anonymisation and disguise mean that either the patient themselves or others would be likely to recognise the patient, explicit consent is required by the UK GDPR.

Ethical considerations for teaching and writing

The general ethical considerations in play for any registrant deciding whether or not to write (or teach) about their patient have been summarised above. **This Guidance recommends that the decision to approach a patient for consent to write about them should be arrived at only after careful and detailed thinking by the registrant, together with the supervisor of their clinical work, regarding such considerations.** This question assumes that the therapist has (i) given careful thought to the relevant ethical considerations as noted above; (ii) arrived at a reasonably justifiable decision to write (or deliver a presentation) using clinical material capable of identifying the patient; and (iii) **consent has been sought and obtained from the patient with the registrant further having satisfied themselves that such consent is informed consent and has been freely given.** In such circumstances, the following guidance is offered with a view, generally, to

avoid harm to the patient, and specifically, to respect the dignity and privacy of the patient:

(a) Disguise, pseudonyms, and anonymisation should be used as a matter of course and as much as possible, with all identifying details changed except where to do so would change materially the substance of what is sought to be conveyed, and the rationale in support of the particular disguise/anonymisation recorded;
(b) In the case of an oral presentation of clinical material disguised as in (i), such presentation should only be given in a closed professional learning context where the public are not admitted and with a clear prohibition against further disclosure or recording of any information relating to the patient;
(c) In the case of a written presentation for training purposes (e.g., a qualifying paper) verbatim material should be limited and highly relevant to the theoretical or clinical argument and (i) paper copies of the written work provided to the relevant training committee should be numbered with an explicit prohibition against further copying or circulation and post-qualification should be returned to the trainee for shredding or other form of secure destruction; (ii) digital copies (also with an explicit prohibition against further copying or circulation) should be encrypted or password-protected and post-qualification should be securely deleted.

It is implicit in the above analysis that, even where there is consent to the use of clinical material capable of identifying a patient, so that there is compliance with the requirements of the UK GDPR, this Guidance recommends an approach to the use of such material which is highly attentive to the interests of the patient. It follows that, in the case of written publications other than those for training purposes (journal papers, book chapters, books, newspaper articles, blogs, policy papers/briefings), and oral presentations either open to the public or disseminated to the public (using broadcasts, podcasts or any other medium), this Guidance recommends that registrants who wish to present a clinical case choose between:

(a) Using clinical material with sufficient anonymisation and disguise that no-one including the patient would be likely to recognise themselves; or
(b) Using a composite case study (composed of partly factual/partly fictional clinical material) which is explicitly described as such.

In (a), although the information relates to an individual patient, the use of anonymisation/disguise means they are not identifiable. In (b), a fictional patient, who is the product of the therapist's imagination and clinical know-how and experience, is being presented (or written about) and specifically described as such, so that there is a clear disclaimer at the outset that no individual living patient is to be identified as the subject of this fictional case study. In both (a) and (b), the requirements of UK GDPR do not apply **AND** the dignity and privacy of the patient are respected.

Record-keeping

As a first principle, and consistent with the guidance set out above, the BPC recommends that in order to protect patient confidentiality records of psychoanalysis and psychoanalytic or psychodynamic psychotherapy should be kept to a minimum. A minimum record would include:

- The patient's name, address (either physical or email, or both) and telephone number and dates of attendance at sessions (specifically and at the very least the date treatment began, how frequently the patient was seen, and when treatment ended).
- Emails and other forms of correspondence between patient and registrant.
- Correspondence between the registrant and other professionals involved in the patient's care.
- Patient consent.
- The fact of presentation at supervision or consultation.
- In particular cases where risk is significant, risk-related clinical decisions and the reasons for them, together with any relevant discussions with supervisors and other professionals (e.g., psychiatric colleagues) and agencies.
- Patient consent (specifically relevant to risk) in particular cases where risk is significant.
- Where particular safeguarding issues arise, either with respect to minor children or vulnerable adults, a detailed account of those issues.

Process notes carrying identifying details would form part of the record. Registrants therefore are advised to keep process notes completely anonymized and separate (from other documents forming part of the record). Such notes should be destroyed as soon as possible after they have ceased to be useful. The BPC recommends that records are kept for a period of six years following the termination of treatment, but this is subject to retention being justifiable in accordance with the requirements of UK GDPR referred to earlier. Registrants need

to be aware of UK GDPR directives particularly with reference to Subject Access Requests.

The location of records and how to access them should be specified in the registrant's professional will, allowing clinical executors to deal with patient needs promptly and efficiently in the event of the registrant's incapacity or death.

Telephone and online therapy

The BPC recognises that telephone or online therapy are valid and at times necessary ways of providing therapy where someone is not able to have it in person. It recognises that there are specific confidentiality issues raised using the telephone or online video/voice over the internet and suggests the following to help manage this:

- Face-to-face therapy is the preferred option, where possible and safe. This may mean referring a patient to another practitioner.
- Registrants should undertake CPD in the practice of telephone and online therapy either before beginning therapy or as soon as possible afterwards.
- Registrants should:
  - request that their patients are in a confidential space when participating in telephone or online therapy and should consider ending the session if this is not the case;
  - use an online platform that utilises end-to-end encryption and does not store sessions on their servers, ideally one that meets the Health Insurance Portability and Accountability Act (HIPAA) requirements (as these US regulations are considered the 'Gold Standard') and ensure that they apply all security updates immediately and all other updates as soon as possible; all meeting invitations and passwords should be kept securely; virtual waiting rooms should be enabled;
  - give guidance to patients about the minimum computer equipment needed to do online therapy safely, including the need to adjust internal settings in the operating system to remove automatic sharing of data, as set out in the Information Commissioner's Office guidance https://ico.org.uk/for-the-public/online/ . The use of a Virtual Private Network (VPN) which anonymously routes internet traffic should also be encouraged;
  - keep their computer's operating systems, anti-virus and anti-spyware programs up to date; they should use firewalls and, ideally, a VPN. The

computer used for online therapy should not be shared with anyone else, including family; they should advise patients to do likewise;

- have information about how to access a named medical practitioner who will take responsibility for the patient's care, including referral to mental health services. Language issues will need to be taken into account if the patient is in a non-English speaking country.

- Registrants should ensure they are explicitly insured for the practice of telephone or online therapy, including any work internationally.
- Registrants should be aware of the risks to themselves and their patients – if any - of offering therapy in countries where they are not lawfully allowed to do so.