Guiding Principles on using personal information when considering concerns

Author(s)	Kirsty Burns /Jo Shaw
Date of last update	May 2018
Version	2.0
Date for review	May 2020

Contents

Overview

1 Disclosure of personal information can be justified provided we act in accordance with the principles outlined below.

2 We should ensure that at all times we only disclose information that is **necessary** and **proportionate** to the purpose of disclosure (i.e. the information is relevant to enable the doctor, employer, expert, etc.) to understand the allegations so that they can fulfil their function.

Necessary

The processing (ie. disclosure) of the data must be necessary for the particular purpose, which cannot be achieved by some other reasonable means.

Proportionate

For disclosure to be proportionate, it must be restricted in its application and effect. For example:

- **Doctor** – sufficient information to enable them to comment on the concerns and properly answer the allegations. The doctor may request un-redacted identifying information, if we have redacted it, which we should consider on a case by case basis with input from legal. See the [insert link to operational guidance] for more details.
- **Expert** – sufficient information to assess the care provided, e.g. date of birth and medical history. The expert does not necessarily need to know the address or NHS number of the patient.
- **Employer** – sufficient information to understand the nature of the allegations which may simply be a brief description rather than any documentation if they are a previous employer. More information is likely to be needed to be disclosed to a doctor's current employer or the employer where the incident took place.

3 The same principles should be considered when requesting information. We should only ask for information that is necessary and relevant for our investigation. The medical records guidance sets out key considerations when requesting information.

4 The redaction guidance defines what we expect from any given party and the information they need to fulfil that role.

5 The redaction guidance includes a matrix of what type of information is necessary and proportionate for the different parties to the case.

Handling personal information

6 Whenever we handle (or process) 'personal information about individuals, we must satisfy the legal requirements under data protection law, Article 8 of the European Convention on Human Rights ('ECHR') and the law as to breach of confidence. In practice, the legal considerations around handling personal information primarily arise when we seek to disclose data externally to third parties.

Data protection law

7 The European General Data Protection Regulation (GDPR) came into force on 25 May 2018 and replaces the Data Protection Act 1998 (DPA). Previously, under the DPA, the GMC relied on consent as the main legal basis for processing personal information (known as 'personal data') under data protection law. Although, under the GDPR, consent remains a lawful basis for processing personal data, the GDPR includes a stricter definition of consent [1]. The GDPR[2] and supporting ICO Guidance[3] now make clear that valid consent will be hard to establish where the data controller is a public authority and there is a clear imbalance of power between the data controller and the data subject, such that the data subject does not have a genuine choice about how their personal data will be handled.

8 The GMC is a public authority for the purposes of the GDPR and there is an imbalance in power between GMC and data subjects, so it is very difficult to say consent is freely given in the majority of circumstances in which information is shared in a fitness to practise context. Therefore, as a general rule, we do not rely on consent as a processing condition under the GDPR when exercising our core statutory functions. We must identify other lawful bases for processing personal data under the GDPR, as well as complying with

[1] 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. (Art. 4(11).

[2] 'In order to ensure that consent is freely given, consent shall not provide a valid ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.' (Recital 43)

[3] The draft guidance has not yet been finalised. It is available at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

the requirements of the law as to breach of confidence and ensuring any possible interference with Article 8 ECHR rights is justified.

Article 8 of ECHR

9 Disclosure of personal information without consent is likely to constitute an interference with an individual's right to respect to private life under Article 8(1) of the ECHR. However, an interference is not unlawful if it can be justified as being necessary, proportionate and for a legitimate aim under Article 8(2) or where it is pursuing a statutory function (e.g. fitness to practise investigations).

10 In order for the disclosure to be justified under Article 8(2), we should inform the individual of the use of their personal information. However, there would be no such obligation if notification was impracticable, or undesirable for some reason of public interest.

Duty of confidence

11 The GMC will also owe a duty of confidence towards individual patients, in relation to information that it holds about the health, and medical treatment, of those patients. This includes information we hold relating to the health and medical treatment of a doctor whose health we are investigating. Disclosure of such information without patient consent will constitute a breach of confidence. However, the GMC may be able to disclose information in relation to which it owes a duty of confidence, without consent, where there is statutory authority for the disclosure, or where there is a sufficient public interest in the disclosure.

12 The definition of consent in the context of breach of confidence is less rigorous than under the GDPR, for example implied consent would be sufficient to justify obtaining or disclosing confidential information. While as a general approach, the GMC will no longer rely on consent as a processing condition under the GDPR, in some parts of our fitness to practise processes, consent to share information may still be needed to override any duty of confidence. For example, in the context of disclosure of information between a doctor's healthcare professional and GMC medical examiner.

13 See Legal Framework section below for further details.

What is a data subject?

14 A data subject for data protection law purposes is an individual who is the subject of personal data; it is the person whom the particular data is about. It does not include an individual who has died. (Please note there are other constraints to disclosure of information about individuals who have died. They are still covered by the duty of confidence we owe to patients[4] – see paragraph [23], page 10).

15 The most common data subjects we encounter in fitness to practise procedures include patients or their families, other complainants like the doctor's work colleagues (who are not the doctor's employer) and witnesses.

What is Personal Data?

16 Personal data is data which relates to an identifiable *living* individual **who can be identified directly or indirectly[5], either**:

- from that data; or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

17 Identifying information in fitness to practise procedures will include information such as an individual's name, date of birth, address, NHS number etc.

18 As a general guide:

- Where the ability to identify an individual partly on the data held and partly on other information (not necessarily data), the data held will still be personal data. For example we may hold records which do not contain a patient's name but do contain their NHS number. The record held is still personal data as the NHS number can be used to identify the individual concerned.
- While a popular name by itself may not identify an individual, a name combined with other information (such as an address, a place of work, or

[4] *Lewis v Secretary of State for Health & Anor* [2008] EWHC 2196 (QB)

[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

a telephone number)…will usually be sufficient to clearly identify an individual'[6].

- There may be circumstances where the data we hold enables us to identify an individual whose name we do not know and we do not intend to find out.

19 Special category data is personal data which is more sensitive, and so needs more protection[7]. For example, personal data relating to health, such as medical records.

20 Where it is not possible to identify a living individual from the data, then this is not considered to be 'personal data'. One way in which it is possible to remove identification of an individual is by anonymisation. Further information concerning the details that should be redacted can be found by reviewing the redaction guidance. The ICO has also produced a guidance document setting out ways in which organisations can effectively anonymise data[8].

What is processing?

21 'Processing' is the obtaining, recording or holding of information or data or carrying out any operation or set of operations on the information or data including[9]:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- **disclosure of the information or data by transmission, dissemination or otherwise making available**; or
- alignment, combination, blocking, erasure or destruction of the information or data.

---

[6] Paragraph 24 of the Opinion of Advocate General *Tizzano in the Lindqvist case (Bodil Lindqvist v Aklagarkammaren i Jonkoping* – Case Commissioner-101/01 – European Court of Justice) delivered on 19 September 2002. See also the cases of *Durant v Financial Services Act* [2003] EWCA Civ 1746; and *Edem v IC & Financial Services Authority* [2014] EWCA Civ 92(paragraph 20).

[7] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

[8] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

This guidance will be focussing on the processing of information by way of **disclosure** to third parties.

Legal Framework

22 Disclosure occurs at multiple stages of our fitness to practise proceedings. There are various provisions under the Medical Act 1983 ('the Act') and in the Fitness to Practise Rules 2004 ('FTP Rules') relating to disclosure, for example:

- Sections 35A(2) and 35B(1) of the Act; the duties placed on the GMC to obtain details of the practitioner's employer/s and to notify a practitioner's employer/s following a decision to carry out an investigation.
- Section 35B(2) of the Act; the power to disclose information to third parties where it is the public interest to do so.
- Rule 7(1)(b) of the FTP Rules; the duty to disclose to the doctor copies of documents received by the GMC which support an allegation.

Disclosing (processing) information

23 Personal information can be disclosed to a third party where there is a legal basis for processing the information under data protection law and we can defend any possible breach of the common law duty of confidence and any possible interference with Art 8 ECHR rights.

24 These legal considerations can be summarised as follows:

- the data subject's rights under the GDPR)

  The GDPR is based around six data protection principles and provides a range of rights for individuals. The principles state that personal data must:

  - be processed lawfully, fairly and in a transparent manner
  - be processed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes
  - be adequate, relevant and limited to what is necessary in relation to the purposes
  - be accurate and up to date

- not be kept for longer than is necessary
- be secure.

The first principle of the GDPR states that data must be processed lawfully and fairly. This means:

a. information must not be processed in a way that breaches either statute or common law. For example, if disclosing information would be a breach of the common law duty of confidentiality, it would also be unlawful under the Act

b. personal information must be handled in ways that are transparent and in ways they would reasonably expect.

One or more of the conditions for processing in Article 6 (for all personal data) and Article 9 (for special category data, which includes health data) to the Act must also be met for the processing to be fair and lawful.

In all cases where personal data is processed, at least one of the conditions set out in Article 6 must be met. The conditions most likely to be relevant to the GMC are that:

- the data subject has given consent (Article 6, paragraph 1(a)
- the processing is necessary because of a legal obligation that applies to the data controller (except an obligation imposed by a contract) (Article 6, paragraph 1(c))
- the processing is necessary to protect the vital interests of the data subject (Article 6, paragraph 4(d))
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6, paragraph 1(e))
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party (Article 6, paragraph (f)).

Where ‘special category data’ are being used, at least one of the conditions in Article 9 must also be met. Information on a patient’s health record is likely to be ‘special category data’ for the purposes of the GDPR.

The conditions most likely to be relevant to the GMC are that:

- the data subject has given explicit consent (Article 9, paragraph 2(a))
- the processing is necessary to protect the vital interests of the data subject or another person in a case where the data subject is physically or legally incapable of giving consent (Article 9, paragraph 2(c)
- the processing is necessary for reasons of substantial public interest (Article 9, paragraph 2(g))
- the processing is necessary for reasons of public interest in the area of public health (Article 9, paragraph 2(i))

The Data Protection Act 2018 makes further provision as to how the GDPR operates in the UK and sets out more specific requirements which must also be met when a data controller is relying on the public interest in Article 9.

- the individual’s right to respect for private and family life under Article 8(1) of the ECHR

Article 8(1) of the ECHR provides that everyone has the right to respect for private and family life, home and his correspondence. This covers medical records and any other information which contains personal data (such as name, address, date of birth). The disclosing of personal data without the consent of the individual about whom that data relates is likely to constitute an interference with that individual’s right under Article 8(1). Any such interference is unlawful unless it can be justified under Article 8(2) as being necessary, proportionate and for a legitimate aim under Article 8(2) or where it is pursuing a statutory function (e.g. fitness to practise investigations).

Where records are completely anonymised and there is no way of identifying the patients and it is not necessary to identify them then it is questionable as to whether Article 8(1) would be engaged at all.

If the disclosure is fair and lawful in accordance with the GDPR it is highly likely that it will be a necessary and proportionate interference with an individual's Article 8 rights. However, even where consent is not a lawful basis for processing data under the GDPR, in order to avoid any risk that the GMC would be acting contrary to a person's Article 8 rights, it is important to notify the data subject about how we will handle their data and give them an opportunity to let us know if they have any concerns or specific requests about how their information will be used.

- our duty of confidence

The GMC owes a duty of confidence towards individual patients (and, unlike under the GDPR, this includes deceased patients), in relation to the information it holds about the health and medical treatment of those patients. This includes information we hold relating to the health and medical treatment of a doctor whose health we are investigating. Disclosure of such information in the absence of consent will be considered to be a breach of confidence. However this breach of confidentiality can be overridden by the GMC's statutory responsibilities to disclose or obtain information or where there is a strong public interest in doing so (see paragraph 21 above).

If there is a legal basis for disclosure under the GDPR, in the absence of consent, then it is likely that any breach of confidentiality will be overridden by GMC's statutory responsibilities or the public interest in obtaining or disclosing information.

25 The case of *General Dental Council v Savery and others* [2011] EWHC 3011 (Admin) considered whether the disclosure of patient information between different individuals within the GDC for the purpose of the GDC's fitness to practise functions without patient consent was lawful. The Court held that:

- Common law confidentiality obligations were overridden by the GDC's statutory duties of disclosure arising from the legal regime governing the GDC's fitness to practise functions.

- There was no breach of the DPA (as was in force at the time). Disclosure was necessary for the exercise of functions conferred by or under an enactment. The conditions in Schedule 2 paragraph 5(b) and Schedule 3 paragraph 7(b) to the DPA were satisfied.

- Disclosure without consent was a breach of Article 8(1) requiring justification under Article 8(2). However, in the circumstances the disclosure would be justified: it was "in accordance with the law" within the meaning of Article 8(2), and it was necessary and proportionate.

- Arguably, in order for the disclosure to be justified under Article 8(2), the GDC was required to inform patients of the use to be made of their records. However, there would be no such obligation if notification was impracticable, or undesirable for some reason of public interest. Where prior notification was impossible, then particular care should be taken to ensure that disclosure or use of the information was for proper purposes.

26 These principles apply in a similar way to the exercise of the GMC's statutory duties of disclosure under the legal regime governing the GMC's fitness to practise functions.

Telling individuals how we will use their personal information

27 Before disclosing an individual's personal information, we should inform them how it will be used in our fitness to practise processes and give them an opportunity to let us know if they have any concerns or specific requests about that use. Although we may choose to pursue an investigation using their personal information in any event, we need to have notified the individual of our intention to use their personal information and sought their views, unless it is impracticable or undesirable to do so for public interest reasons. Where the individual raises concerns or makes a specific request about the use of their information we will need to take this into account.

28 This principle applies regardless of where the information comes from. That is whether it is from a member of the public, or from a third party who is not the data subject, such as an employer, the police or other public body.

29 In a trust referral, or where a third party complains on a patient's behalf, we may be told by the person complaining that they don't think it is appropriate for us to contact the patient and tell them that we are using their personal information. In those circumstances we should seek as much information as possible about the reasons why including, where relevant, details of any perceived risk of harm to the patient. A decision should then be taken as to whether or not to contact the patient. Any decision not to notify an individual about the use of their personal information should be clearly recorded.

30 When considering this issue, staff should follow the principles set out in the following guidance (note: this list is non-exhaustive):

- Guidance for decision makers on using personal information where an individual raises concerns or makes a request
- Anonymous / confidential complaints
- Guidance to staff on communicating with patients and the people close to their care
- DBS guidance

Assessing concerns or requests raised by an individual about the use of their personal information

31 Any concerns or requests raised by an individual about how their personal information will be handled by the GMC will require a decision to be made by an Assistant Registrar. The decision maker will need to consider whether it is necessary and proportionate to use the information in the proposed form for the intended purpose, in light of the views expressed by the individual. The extent of the interference with the individual's rights under the GDPR and Article 8 of the ECHR and the duty of confidence owed to them must be balanced against the GMC's statutory obligation to investigate fitness to practise concerns and its overarching objective to protect the public. More detail is set out in the **Guidance for decision makers where an individual raises concerns or makes a request about the use of their personal information**.

32 There may be cases where we write to an individual to inform them about how their personal information will be used in our fitness to practise processes and despite them not replying to notify us of any concerns or requests, it will be

appropriate to raise an Assistant Registrar decision rather than automatically proceeding to use their personal information. This is likely to be most relevant where the individual we are writing to is potentially vulnerable and / or the case is of an extremely sensitive nature. Investigations staff should discuss these cases with an investigation manager to agree on appropriate next steps, including whether an Assistant Registrar decision is needed.