General Medical Council

Using personal information in the fitness to practise process for Physician Associates and Anaesthesia Associates

Table of Contents

Date of publication: December 2024

Last updated: December 2024

Introduction

1. Personal information is information that could be used to identify a living person, either directly or indirectly. This guidance sets out our approach to using personal information in fitness to practise and making decisions about such use.

2. The guidance is split into two main sections, Part A and Part B. Part A sets out the guiding principles when using personal information. Part B supports the Regulator to reach fair and consistent decisions about whether we should proceed to disclose or obtain personal information when the data subject has made a request or raised a concern about such use.

Part A: Guiding Principles

Introduction

3. Use of personal information can be justified provided we act in accordance with the following principles:

a. We must have appropriate regard to our legal obligations

Whenever we 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, although they also apply where there are concerns or requests about us obtaining personal information. More detail about the relevant legal obligations is included later in the guidance, including a glossary of key technical terms at the end.

b. The data subject should be given the opportunity to raise objections about how we'll use their information

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 use 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.

c. Any concerns or requests must be considered

Where concerns have been raised or requests made about our use of personal information, we will need to take this into account. This is regardless of whether the information has come from the data subject, i.e. who the information is about, or from a third party who is not the data subject but is acting on their behalf, such as an employer or public body.

d. Any disclosure of information should be necessary and proportionate

We should always ensure that we only disclose information that is necessary and proportionate to the purpose of disclosure i.e. the information shared is necessary for the particular purpose, which cannot be achieved by some other reasonable means, to enable the Physician Associate (PA) or Anaesthesia Associate (AA), employer, expert, etc. to understand the concerns so that they can fulfil their specific function.

Data protection law

4. The UK General Data Protection Regulation (GDPR) sits alongside the Data Protection Act 2018 (DPA), and together they represent the primary data protection legislation in the UK. The GDPR[*] and supporting ICO Guidance[†] 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. This regulation does not apply to the personal data of those who are deceased[‡].

5. The GMC is a public authority for the purposes of the GDPR and there is therefore an imbalance in power between the GMC and data subjects, so it may be difficult to say consent is freely given in most 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 should identify other lawful bases for processing personal data under the GDPR, as well as complying with 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

6. Article 8(1) of the ECHR provides that everyone has the right to respect for private and family life, home and correspondence. This covers medical records and any other information which contains personal data (such as name, address, date of birth). 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.

7. 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

[*] '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)

[†] 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

[‡] This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons. (Recital 27)

obligation if notification was impracticable, or undesirable for some reason of public interest.

8. Where records are completely anonymised and there is no way of identifying the data subject then it is unlikely that Article 8(1) would be engaged.

9. 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.

Duty of confidence

10. The GMC also owes a duty of confidence towards data subjects in relation to confidential information we hold about them obtained as part of our fitness to practise investigations. For investigations about PAs and AAs this includes patients, the PA or AA and others. For patients, we owe a duty of confidence in relation to information we hold about their health and medical treatment. This includes information we hold relating to the health and medical treatment of a PA or AA. Unlike the GDPR, our duty of confidence also applies to deceased data subjects. Disclosure of such information without consent will constitute a breach of confidence, unless there is statutory authority for the disclosure, or where there is sufficient public interest in the disclosure.

11. 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 PA or AA's healthcare professional and GMC health examiner.

12. 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 the GMC's statutory responsibilities or the public interest in obtaining or disclosing information.

Part B: Making a decision on whether to proceed to use personal information

Introduction

13. Any use of personal information where concerns have been raised or requests made about our use will require a decision as to whether the proposed use is necessary and proportionate in spite of these.

14. In practice this primarily arises when we seek to disclose personal information externally to third parties and need to consider if, despite any concerns or requests, the disclosure is necessary and proportionate. However, an individual can also raise concerns or make requests about us obtaining personal information. In this instance, we will need to consider if, despite any concerns or requests, it is necessary and proportionate to go ahead and use our powers to request that information.

15. When making these decisions, our duty to protect the public must be balanced against the extent of any likely interference with the individual's rights under data protection law, Article 8 of the ECHR and the duty of confidence owed to them. More detail about these rights is available in the above guiding principles section.

16. A good decision about whether we can proceed to use an individual's personal information despite any concerns or requests should also meet our fitness to practise decision making principles. These state that all decisions should protect the public and be proportionate, transparent, and fair. These principles are explained further in the explanatory publication *Decision making principles in fitness to practise (Physician Associates and Anaesthesia Associates).*

Special considerations

17. Concerns or requests can only be raised or made by the data subject or by someone with authority to act on their behalf. This means that if a complainant is writing on someone else's behalf, we either need confirmation of the authority of the complainant to express views on the data subject's behalf, or we need to communicate directly with the data subject.

18. We should assume that the data subject has the capacity to express views about how we use their personal information. However, if there is clear information that suggests the data subject does not have the capacity to understand how we are going to use their personal information and / or make us aware of any concerns or requests about that use, we may need to communicate with someone with the authority to communicate on their behalf. To consider this, the Regulator should refer to the *Guidance to staff on communicating with patients who experience barriers to engaging with us and the people*

close to their care.

19. If the individual is deceased, they are not a data subject so data protection legislation and Article 8 of the European Convention on Human Rights ('ECHR') will not apply. However, Article 8 rights may still be owed to a family member and we are still bound by a duty of confidence so these will still need to be considered before we use their personal information.

Making a decision

20. To determine whether to proceed to use an individual's personal information, the Regulator should consider the following questions:

What is the assessment of risk arising from the information received about the PA or AA's behaviour, performance or impact of a health condition?

21. The guidance *Decision on whether regulatory action is required* guides decision makers on how to reach a view on the overall risk that a PA or AA poses to public protection, if any, based on where on the spectrum of seriousness the information received lies, the impact of any relevant context and how the PA or AA has responded. The Regulator will have already undertaken an assessment of risk (or potential risk depending on their current stage in the fitness to practise process).

22. In order to decide whether we should proceed to use the personal information despite any concerns raised or requests made, a number of factors set out below should be weighed and balanced against the assessment of risk of the PA or AA's behaviour, performance, or impact of a health condition.

23. The weight to be attributed to each of the factors should be assessed by the Regulator on a case-by-case basis, however the higher the assessment of risk, the more weight any factors in favour of using the information and the less weight any factors against using the personal information will have. Conversely, where the information received indicates that the PA or AA poses a low risk to public protection, the less weight any factors in favour of using the information and the more weight any factors against using the information will have. The considerations of each factor are likely to have a cumulative impact, with no single one being decisive.

Are there factors weighing in favour of using the personal information?

24. The factors weighing in favour of using the personal information may include:

a. **It would not be possible to conduct a fair assessment of the information received about the PA or AA if the individual's personal information is not used.**

   Having quality evidence from a range of sources will support fairness in decision making. Fairness is explained further in the explanatory publication *Decision making principles in fitness to practise (Physician Associates and Anaesthesia Associates)*.

b. **The concern raises an important point of practice or principle/ethics.**

   This type of concern can have a higher impact on public confidence, one of the three parts of public protection. Consideration should therefore be given to if the information about the PA or AA raises an important issue relating to the standards, values and principles expected from PAs and AAs. Good Medical Practice sets out the principles, standards of care and professional behaviour expected of all PAs and AAs registered with us and is an ethical framework, which supports PAs and AAs to deliver safe care to a good standard.

Are there factors weighing against using the personal information?

25. The factors weighing against using the personal information may include:

a. **The GMC would be incapable of evidencing the concerns without the cooperation of the individual.**

   Consideration should be given to the GMC's ability to rely on alternative material to evidence the concern(s). If the data subject is the main witness and without their cooperation it would be difficult to establish an evidence base from which to assess whether the PA or AA's fitness to practise is impaired, use of their personal information is unlikely to be justified where they have raised concerns or made requests about that use.

   Where there has been a third-party investigation, the substantive reason(s) for the outcome should be established. This is likely to be relevant to the consideration of whether the GMC is capable of evidencing the concern(s) some other way. The standard of proof we apply (the balance of probabilities) is lower than the standard of proof in criminal cases (beyond reasonable doubt) which may mean we can evidence a matter for the purpose of fitness to practise proceedings that did not result in a conviction in a criminal case.

b. **Any risk to the individual if the GMC were to proceed to use, and in particular disclose, their personal information.**

   The degree of the harm should be considered. It is likely that only a risk of significant harm, rather than, for example distress, could weigh substantially against a wider risk to patients and the public should the GMC not use the personal information to

support the assessment of a concern. Where the individual has requested confidentiality, we should weigh the reason(s) for this against the public interest.

On balance, is the proposed use of the personal information necessary and proportionate?

26. If the Regulator is not satisfied that disclosing or obtaining the personal information is necessary in order to fulfil our duty to protect the public, then the proposed use of the personal information should not go ahead. More information about our public protection duty is available in the explanatory publication *Decision making principles in fitness to practise (Physician Associates and Anaesthesia Associates)*.

27. If the Regulator is satisfied that disclosing or obtaining the personal information is necessary in order for the GMC to fulfil its duty to protect the public, the resulting interference with the individual's rights is likely to be necessary and proportionate, provided we take all reasonable steps to minimise any such interference. This includes identifying any measures to ensure that the information disclosed is only what is needed to allow the recipient to fulfil their required function, such as redaction. So for:

- a **PA or AA**, the information shared must be sufficient to enable them to comment on the information received about their behaviour, performance or impact of a health condition, including providing any relevant context and / or insight and remediation they have undertaken.
- an **Expert**, the information must be sufficient to enable them to assess the care provided by the PA or AA.
- an **Employer**, the information must be sufficient to understand the nature of the concern.

28. 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.

29. Where an individual has raised concerns or made a request about the use of their personal information, they should be informed of any decision to proceed to use their personal information, unless there is a good reason in the particular circumstances not to do so; for example, it is impracticable or undesirable for some reason in the public interest.

Glossary

What is a data subject?

30. A data subject 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[*] – see paragraph 19).

31. The most common data subjects we encounter in fitness to practise procedures about PAs and AAs include the relevant PA or AA, patients or their families, complainants and witnesses.

What is personal data?

32. Personal data is data which relates to an identifiable living individual who can be identified directly or indirectly.

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

- 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.

34. 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. This is the case even if we do not intend to use the data to identify the individual.
- 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 a telephone number) will usually be sufficient to clearly identify an individual'[†].

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

[†] 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

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

36. 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.

What is processing?

37. '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[†]:

- 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.

cases of *Durant v Financial Services Act* [2003] EWCA Civ 1746; and *Edem v IC & Financial Services Authority* [2014] EWCA Civ 92(paragraph 20).

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