General Medical Council

Using personal information in the fitness to practise process (Doctors)

Table of Contents

Date of publication: May 2025 (in effect from 30 May 2025)

Last updated: May 2025

Introduction

1. Personal information is information that could be used to identify a living person, either directly or indirectly. During all stages of the fitness to practise process, the Regulator* will need to use personal information to be able to assess whether a doctor may pose / poses any current and ongoing risk to public protection.

2. References made to 'public protection' throughout this guidance refer to the Regulator's legal duty to protect the public which is split into three distinct parts. It means the Regulator must act in a way that:

   - protects, promotes and maintains the health, safety and wellbeing of the public,
   - promotes and maintains public confidence in the professions, and
   - promotes and maintains proper professional standards and conduct for members of the professions.

   The publication *Decision making principles in fitness to practise (Doctors)* explains this legal duty in more detail.

3. The purpose of this guidance *Using personal information in the fitness to practise process (Doctors)* is to support the Regulator to reach fair and consistent decisions about whether to proceed to disclose or obtain personal information when a data subject has made a request or raised a concern about the use of their information for the purpose of assessing a doctor's fitness to practise.

   - Part A sets out the guiding principles that apply when using personal information in the fitness to practise process.
   - Part B provides guidance on how to decide whether to proceed to disclose or obtain personal information when a data subject has made a request or raised a concern about the use of their information.

* References to 'the Regulator' mean the GMC and GMC staff who are authorised to make decisions at each stage of the fitness to practise process on behalf of the GMC.

Part A: Guiding Principles

4. Use of personal information in the fitness to practise process can be justified provided the Regulator acts in accordance with the following principles:

a. Have appropriate regard to relevant legal obligations.

Whenever the Regulator processes personal information about individuals, 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 must be satisfied.

In practice, the legal considerations around handling personal information primarily arise when the Regulator seeks to disclose data externally to third parties, although they also apply where there are concerns or requests about 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 their information will be used.

Before disclosing an individual's personal information, the Regulator should inform them how it will be used in the fitness to practise process and give them an opportunity to say if they have any concerns or specific requests about that use.

Although the Regulator may choose to use their personal information in any event, the individual needs to have been notified of the Regulator's intention to use their personal information and given an opportunity to provide 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 the Regulator's use of personal information, this must be taken into account regardless of whether the information has come from the data subject, i.e. the individual 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.

The Regulator should always ensure that only information that is necessary and proportionate to the purpose of disclosure is shared.

In practice this means the information shared is necessary for the particular purpose of the disclosure, which cannot be achieved by some other reasonable means, such as to enable the doctor, employer, expert, etc. to understand the concerns so that they can fulfil their specific role or function in the fitness to practise process.

Data protection law

5. 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 Information Commissioner's Office (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[†].

6. The GMC ('the Regulator') is a public authority for the purposes of the GDPR and there is therefore an imbalance in power between the Regulator 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, the Regulator does not rely on consent as a processing condition under the GDPR when exercising its core statutory functions. The Regulator 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 the duty of confidence and ensuring any possible interference with Article 8 ECHR rights is justified.

Duty of confidence

7. The Regulator owes a duty of confidence towards data subjects in relation to confidential information held about them obtained as part of the fitness to practise process. For investigations about doctors this includes patients, the doctor and others.

8. For patients, the Regulator owes a duty of confidence in relation to information held about their health and medical treatment. This includes information relating to the health and medical treatment of a doctor. Unlike the GDPR, the 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.

9. 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.

10. As a general approach, the Regulator will not rely on consent as a processing condition under the GDPR. However, in some parts of the fitness to practise process, consent to

[*] '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)

[†] Whilst GDPR does not apply to deceased people, there are still data privacy considerations that organisations have to take in relation to deceased individuals' personal data.

share information may still be needed to override any duty of confidence. This primarily arises in the context of disclosure of information between a doctor's healthcare professional and GMC health examiner.

11. 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 Regulator's statutory responsibilities or the public interest in obtaining or disclosing information.

Article 8 of ECHR

12. 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).

13. 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.

14. For the disclosure of personal information to be justified under Article 8(2), the Regulator 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.

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

16. If the disclosure is fair and lawful in accordance with the GDPR, it is highly likely that it will amount to 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, to avoid any risk that the Regulator would be acting contrary to a person's Article 8 rights, it is important to notify the data subject about how their data will be handled and give them an opportunity to say if they have any concerns or specific requests about how their information will be used.

Part B: Deciding whether to proceed to use personal information

17. Any use of personal information where concerns have been raised or requests made about its use will require a decision to be made as to whether the proposed use is necessary and proportionate.

18. In practice this primarily arises when the Regulator intends to disclose personal information externally to third parties and needs 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 the Regulator obtaining personal information. In this instance, the Regulator will need to consider if, despite any concerns or requests, it is necessary and proportionate to go ahead and use relevant powers to request that information.

19. When making these decisions, the Regulator's legal duty to protect the public must be balanced against the extent of any likely interference with the individual's rights under data protection law, the duty of confidence owed to them and Article 8 of the ECHR. More detail about these rights is set out in Part A of this guidance: *Guiding principles*.

20. A good decision about whether the Regulator can proceed to use an individual's personal information despite any concerns or requests should also meet the fitness to practise decision making principles. These state that all decisions made in the course of assessing a doctor's fitness to practise should protect the public and be proportionate, transparent, and fair. These principles are explained in detail in the explanatory publication *Decision making principles in fitness to practise (Doctors)*.

Special considerations

21. 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, the Regulator either needs confirmation of the authority of the complainant to express views on the data subject's behalf, or to communicate directly with the data subject.

22. The Regulator should assume that the data subject has the capacity to express views about how their personal information is used. However, if there is clear information that suggests the data subject does not have the capacity to understand how the Regulator intends to use their personal information and / or raise any concerns or requests about that use, the Regulator may need to communicate with someone with the authority to communicate on their behalf. To consider whether this is appropriate during an investigation, the Regulator should refer to the relevant section in the guidance *Deciding how to approach evidence collection (Doctors)*.

23. 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 the Regulator is still bound by a duty of confidence so these legal obligations will still need to be considered before the Regulator uses their personal information.

Should the Regulator proceed to use an individual's personal information?

24. To decide 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 / concern about the doctor's behaviour, performance and / or impact of a health condition on their ability to practise safely and effectively?

25. The guidance *Decision on whether regulatory action is required (Doctors)* provides guidance on how to assess whether a doctor poses any current and ongoing risk to one or more of the three parts of public protection. This assessment is made by considering the seriousness of the information received / concern, the impact of any relevant context known about the doctor and / or their working environment and how the doctor has responded.

26. The Regulator may have already undertaken an assessment of risk, or potential risk, depending on the stage in the fitness to practise process the matter is at. If so, this can be used to inform the Regulator's decision about whether to proceed to use the data subject's personal information. However, if this has not already been done, or the evidence available to the Regulator has changed, the Regulator should apply the guidance *Decision on whether regulatory action is required (Doctors)* to reach a view on current and ongoing risk.

27. To decide whether to proceed to use personal information despite any concerns raised or requests made, the factors below should be weighed and balanced against the assessment of current and ongoing risk to public protection arising from the doctor's behaviour, performance and / or the impact of a health condition on their ability to practise safely and effectively.

28. The weight to be attributed to each of the factors should be assessed by the Regulator on a case-by-case basis. The considerations of each factor are likely to have a cumulative impact, with no single one being decisive. But where the information received / concern usually falls at the *higher end of the spectrum of matters that give rise to a question of impaired fitness to practise*, the more weight any factors in favour of using the personal information, and the less weight any factors against using the personal information, will usually have.

However, where the information received / concern usually falls at the *lower end of the spectrum of matters that give rise to a question of impaired fitness to practise*, the less weight any factors in favour of using the personal information and the more weight any factors against using the personal information will usually have.

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

29. The factors weighing in favour of using personal information include, but are not limited to:

a. **It would not be possible to conduct a fair assessment of the information received / concern about the doctor 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 (Doctors)*.

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

   Good medical practice ('GMP') sets out the principles, standards of care and professional behaviour expected of all doctors registered with the GMC and is an ethical framework, which supports doctors to deliver safe care to a good standard, in the interests of patients.

   Consideration should be given to if the information / concern about the doctor raises an important issue relating to the professional standards set out in GMP. Where it does, the matter is likely to have a higher impact on public confidence in the profession.

Are there factors weighing against using the personal information?

30. The factors weighing against using the personal information include, but are not limited to:

a. **The Regulator would be incapable of evidencing the concern(s) without the cooperation of the individual.**

   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 doctor poses any current and ongoing risk to one or more of the three parts of public protection i.e. assess whether their fitness to practise is impaired, use of the data subject's personal information is unlikely to be justified where they have raised concerns or made requests about that use.

   However, consideration should be given to the Regulator's ability to rely on alternative material to evidence the concern(s).

   Where there has been a third-party investigation, including by the police, the substantive reason(s) for the outcome should be established. This is likely to be relevant to the consideration of whether the Regulator can evidence the concern(s) some other way.

   The standard of proof that applies at a Medical Practitioner Tribunal hearing (the balance of probabilities) is lower than the standard of proof in criminal cases (beyond reasonable doubt) which may mean the Regulator 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 Regulator 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, to the individual could weigh substantially against any wider risk to public protection should the Regulator not use the personal information to support the assessment of a concern.

Where the individual has requested confidentiality, the reason(s) for this should be weighed against the public interest.

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

31. If the Regulator is not satisfied that disclosing or obtaining the personal information is necessary to fulfil the legal duty to protect the public, then the proposed use of the personal information should not go ahead.

32. If the Regulator is satisfied that disclosing or obtaining the personal information is necessary to fulfil the Regulator's legal duty to protect the public, the resulting interference with the individual's rights is likely to be necessary and proportionate, provided the Regulator takes 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.

- When disclosing to a **doctor**, the information shared must be sufficient to enable them to comment on the information received about their behaviour, performance and / or impact of a health condition, including providing details of any relevant context about themselves or their working environment and / or evidence of insight and remediation they have undertaken.
- When disclosing to an **expert**, the information must be sufficient to enable them to assess the care provided by the doctor.
- When disclosing to an **employer**, the information must be sufficient to understand the nature of the concern.

33. The Regulatory should consider the approach to redacting information before disclosing it. The Regulator may also want to consider any guidance issued by the ICO which sets out ways in which organisations can effectively anonymise data.

34. 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?

35. 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.

36. The most common data subjects encountered in fitness to practise procedures about doctors include the relevant doctor, patients or their families, complainants and witnesses.

What is personal data?

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

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

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

39. 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, the Regulator 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 the Regulator does 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'[*].

40. 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. The Regulator may also want to consider any guidance issued by the ICO which sets out special

[*] 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).

category data.

41. 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?

42. '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
- alignment, combination, blocking, erasure or destruction of the information or data.