Consultation on Confidentiality: draft guide for consultation

1. The Royal College of General Practitioners (RCGP) welcomes the opportunity to respond to the General Medical Council’s (GMC) consultation on Confidentiality – draft guidance for consultation.

2. The RCGP is the largest membership organisation in the United Kingdom solely for General Practitioners (GPs). Founded in 1962, it has over 52,000 members who are committed to improving patient care, developing their own skills and promoting general practice as a discipline. We are an independent professional body with expertise in patient-centred generalist clinical care.

3. The RCGP would like to thank Dr Ralph Sullivan for his contribution to this submission.

4. The RCGP considers the confidentiality guidance to be a high quality, helpful document. There are, however, some sections where there is scope for refinement to reflect the complex nature of modern general practice. There are also areas in which greater clarity is needed.

The framework for considering when to disclose personal information
5. Paragraph 15 is confusing as currently drafted. It could be interpreted as saying that patients can object to the disclosure of anonymised data from their records when that is not correct. It is not clear that the first three bullets are alternatives, which is the only way to make sense of the statements. The last two bullets, (at the top of page eight) apply in all cases. This paragraph should be written more clearly.

6. Paragraph 16 is too vague as currently drafted. It is not clear whether doctors need to inform every patient about every disclosure, and how doctors are to know what patients reasonably expect. The RCGP supports the sentiment of this paragraph but the paragraph should be written more clearly.

7. Paragraph 18 or 19 should clarify whether a patient who is unable to object or indicate any level of consent (e.g. a patient with a severe intellectual disability who is unable to understand the consent question) can be taken to have given implied consent under clearly defined circumstances.

8. Paragraph 19 should define the term "local clinical audit". The term used to be clear but now it should probably refer to audit within one data controller’s domain (e.g. a single General Practice or NHS Trust). It would not, for example, include audit across a CCG or federation of practices (see also comment on paragraph 46). THE RCGP understands that the Data Protection Act 1998 (DPA) applies to this situation and it might be useful to reference the DPA or mention data controllers.

9. Paragraph 20 is unclear about what this would entail in practice, which is important as informing patients about every disclosure is not practical. The RCGP understands the practical intent of the paragraph to mean using a Privacy Notice or providing detail in an application for registration under the DPA 1998. This paragraph should include further detail to clarify this.

10. Paragraph 24 is unclear with regard to the meaning of “you should satisfy yourself that any disclosure is required by law”. It presumably is not intended to impose a blanket requirement that all disclosures must be required by law. The RCGP takes this paragraph to mean that the doctor has to be sure that any legal justification used to allow a disclosure is valid, or that the doctor should understand the difference between a disclosure that is required by law and one that is permitted by law, where the doctor may decline the disclosure.
11. Paragraph 25 is confusing as currently drafted. It appears to state that even where a disclosure is permitted in law, there has to be another legal permission to disclose the information.

12. Paragraphs 28-34 appear to state that if it is in the public interest, then it is acceptable to disclose identifiable information for indirect care purposes such as research, education, and training, without obtaining the patient’s explicit consent (e.g. if numbers are such that it would be impractical) and without any other legal justification. The paragraph should be rewritten to make clear exactly what doctors would or would not be allowed to do in light of the forthcoming review by Dame Fiona Caldicott and the GMC should consider the findings of her report.

**Direct care uses and disclosure**

13. The RCGP recommends including a subsection on situations where doctors have access to patient information but do not have a right to access it (i.e. no legitimate relationship) or need to ask the patient for consent to view (e.g. health record viewers, such as the Medical Interoperability Gateway in out of hours, Accident and Emergency departments and hospices).

14. The RCGP believes it would be useful to include a statement about the common situation where a general practice partnership is the legal data guardian for patient personal confidential information but does not have a contract with a data processor acting under contract to the Clinical Commissioning Group (e.g. general practice system suppliers through GP Systems of Choice) or under contract to the patient (e.g. a Patient Online Access application on a smartphone or tablet). Currently general practice system suppliers have signed letters to indemnify practices if they cause a privacy breach as a result of professional pressure but other companies in the future may not do so. Currently it is unclear how the GMC would view this scenario if a patient complained.

15. Paragraph 41 includes reference to “shared within the healthcare team”. The RCGP is concerned about the use of this term. Sharing in a practice healthcare team happens when anything is recorded in a patient’s electronic health record and The RCGP does not support preventing a doctor from recording information in the patient’s record if the patient tells them not to.
This could cause issues for the doctor (e.g. if a GP wants to record that a patient has refused admission to hospital but the patient tells the GP not to record that fact. This paragraph could mean that the GP needs to follow the patient’s direction, even though it puts the GP at a medico-legal disadvantage).

16. Paragraph 42 is unclear as to whether “referral” must mean to someone outside the health organisation (e.g. practice) or may include referral within the organisation The paragraph should be rewritten to clarify this.

17. Paragraph 46 should define more clearly “the team that provided care”. The RCGP understands that the DPA (1998) applies to this situation and it would be useful to reference the DPA (1998) or mention data controllers (see also comment on paragraph 19).

**Indirect care uses and disclosure**

18. The GMC should reconsider the structure of this part of the document to make it clearer and more current.

19. The RCGP considers that the three classes of data that the draft guidance uses (anonymised, de-identified and identifiable) are not appropriate. In particular there is no clear distinction between “anonymised data with little risk of an individual being identified” and “de-identified [where] there is still some risk that individuals could be re-identified”. The latter could still be effectively anonymised if the right access controls are in place. The term “effectively anonymised” is increasingly out of date. Data is either anonymised or not, where it is statistical data or patient-level data. The new Information Governance Alliance Report that is being written currently takes the view that any de-identified data may be deemed to be anonymised if it is protected with access controls and other techniques such as encryption to the level that the risk of a patient being identified in the data is negligible.

20. The document should include information about data sharing agreements and contracts. It is very important that doctors have confidence that the purpose that the data is being disclosed for is the only use to which the data will be put and that the recipient will protect the data properly. Doctors should take care not to disclose re-identifiable data to an organisation without confidence in the form of a data sharing agreement or contract that the data will be protected.
21. There are several statements in the *indirect core users and disclosure* section of the confidentiality guidance about patients’ objections being upheld. It may be worth including guidance about whether a single global objection for indirect uses must be followed by doctors, and whether a global objection can be ignored when a patient gives a specific consent, such as for one class of uses or a specific research project. This issue is being considered in detail by Dame Fiona Caldicott and the GMC should consider the findings of her report when it is released.

22. Paragraph 88 is not precise enough and may be misleading. It implies that a doctor could give identifiable data to anyone to de-identify it. There is mention of contracts but it does not say who should hold the contract. The RCGP considers that this paragraph should be re-written to give clear advice about the relevance of the DPA (1998) and the *Health and Social Care Act 2012* (HSCA). There is a major issue on which the confidentiality guidance must provide clarity. General practices do not have a contract with any organisation that is capable of de-identifying data (e.g. the GP system suppliers) and the Health & Social Care Information Centre needs a direction under the HSCA (2012) to require health organisations to disclose identifiable data to them.

23. Paragraph 89 should explicitly state that a doctor must ensure that any disclosure of data for which they are responsible, is covered by a privacy or fair processing notice. The current text implies that a GP might feel they are covered for releasing data obtained from the local hospital if the local acute trust has a privacy notice.

24. Information under the heading *Disclosing information for indirect care purposes from which a patient might be identifiable* (paragraphs 90-109) is not correct as it stands because “might be identifiable” overlaps with “anonymised data” according to the definitions already used. The section should state that where identifiable information or de-identified information is to be disclosed under a data sharing agreement, that does not guarantee that the data will be protected well enough to give confidence that there is a negligible risk that the data will be re-identified.

25. The RCGP considers that the output and opinions of the advisory body should be public and they should be independent of the body seeking the data in the same way that a Caldicott Guardian should be (paragraph 106).
Non-care uses and disclosure

26. Paragraph 112 is unclear as to who qualifies as "an officer of a government department or agency" or as "a registered health professional" in this case. The paragraph should explain this or include a definition in the glossary. There are apparent examples of people who might be included in these groups whom doctors maybe uncomfortable about sharing personal data with only an assurance of patient consent (e.g. an occupational health nurse for a commercial company). It is not clear who can claim to be an “officer” in these circumstances.

Managing and protecting personal information

27. Paragraph 136 says that doctors will not usually be data controllers. This is misleading. There are nearly 40,000 GPs who are data controllers through their partnerships. It would be more accurate to say that "doctors may not be data controllers in their individual clinical roles".

28. Paragraph 140 could include more information about unauthorised access to computers and computer screens and the use of mobile devices and phones to modernise this section. Although the paper records access issues are still valid they are becoming less important compared to digital access.

29. The guidance on records management and retention (paragraphs 144-148) could include a statement that, where the doctor is responsible for data protection, they should ensure that the organisation achieves at least level 2 on the Information Governance Toolkit.

30. Paragraph 144 is not clear on the meaning of “unless you have a management role” for general practices that have systems with security specified by GP Systems of Choice and contracted by their Clinical Commissioning Group. This should be explained.

31. Paragraph 151 includes a requirement to “make sure that patient information is secure when it is stored or transmitted”. As currently drafted, this would prevent doctors using ordinary email or video conferencing (e.g. Skype, FaceTime) communication with patients because it is not possible to make it secure and because data may also be stored in overseas data centres, which is prohibited under the DPA (1998). The RCGP recommends including a statement that "doctors can use ordinary commercial email and video
conferencing systems to communicate with a patient with that patient's consent”.

**Glossary**

32. **Anonymised information**: the definition should be consistent with the DPA 1998 and Information Commissioner’s Office definition of “negligible risk” or re-identification. The definition should note that the risk of re-identification depends on more than the data. It includes the access controls and having a data sharing agreement in place.

33. **De-identified information**: this definition is not correct as currently drafted. Pseudonymisation is only one technique that can be used for de-identification. The rest of the paragraph contains other errors that should be resolved. The RCGP suggests that GMC consult Malcolm Oswald who is the author of the Information Governance Alliance paper for the HSCIC on anonymisation of data as an expert in this area.

34. **Identifiable information**: This definition is not helpful. De-identified data may be identifiable (e.g. age and four characters of the post code will identify some people and some four character districts have less than one hundred people living there). The difference between personal data and identifiable data should also be explained.

35. It might be helpful to define the term “personal confidential information”. Not all information that a doctor holds or might disclose is confidential.

**Legal Annex**

36. The last principle of the DPA (1998) should be expressed in more detail. There are countries where personal confidential information can be transferred legally, which is not what the confidentiality guidance says.