GMC consultation

Confidentiality guidance: your views (ICO response submitted online)

We give doctors guidance on dealing with confidentiality issues, together with case studies to show how the guidance works in practice. We are currently reviewing how we do this.

We’d like to know what you think of the guidance and how we could improve it. The responses we receive will help us to redraft the guidance, which we will be consulting on during 2015.

Our professional guidance for doctors describes what good medical practice looks like. It sets out the professional values, knowledge, skills and behaviours expected of all doctors, in all specialties, across the four countries of the UK. Doctors must use their judgement to apply the principles to the situations that they face in practice.

In our confidentiality guidance, we advise doctors on the ethical and legal principles that underpin the collection and use of information about patients. We do not set detailed clinical standards, and we are not able to provide technical or detailed operational advice (for example, about IT design or software security). Other bodies such as the medical royal colleges, and departments of health, give guidance of this kind.

Question 1. Given the purpose and scope of our guidance, do you think there is anything missing from it? If so, what? [ ]

- The content of guidance on confidentiality is generally not something for the ICO to comment on as the regulator responsible for the Data Protection Act 1998 (DPA). We do however wish to comment about the context that the guidance will apply in. The legal regime which applies to confidential information operates in parallel with the DPA, and we are keen to ensure that the guidance acknowledges that doctors must take the requirements of the DPA into account as well as those of confidentiality, where the information processed is personal data or sensitive personal data. Whilst the guidance does mention the DPA as legislation that needs to be considered, there is a risk that some doctors might see the guidance as the complete approach to managing personal health information and could disregard the requirements of the DPA. Of course we do recognise that the guidance is not intended to cover the requirements of the DPA as its focus is confidentiality, but we would suggest it is important that the guidance makes a clear and explicit reference to the fact the organisations will also have to take into account the requirements of the DPA where the information processed is personal data or sensitive personal data.
We don’t give doctors legal advice or provide a guide to the law. But we do aim to identify the ethical and legal issues that will help doctors to make decisions that respect the privacy, autonomy and choices of patients, as well as benefiting the wider community. We want doctors to be confident that they are acting within the law when they follow our guidance, even if they might need to get specific legal advice in some cases.

We also want the guidance to be accurate and clear.

**Question 2.** Is anything in the guidance inconsistent with the law? If so, what?

- There are some general inconsistencies between the approach to consent taken by the common law of confidentiality and the approach taken by the DPA. This general difference in approach is detailed in our response to question 8.

**Question 8.** Is there anything else you would like to tell us about our guidance?

Disclosures for local clinical audit

In paragraph 7 the guidance states "You should make sure that information is readily available to patients explaining that, unless they object, their personal information may be disclosed for the sake of their own care and for local clinical audit." We are unsure what exactly is meant by "local clinical audit" but from a DPA point of view, whether sensitive personal information should be disclosed for the purposes of local clinical audit without explicit consent might depend on whether the audit is carried out internally within the practice or whether it is carried out by an external team (the latter of which might be outside of the reasonable expectations of patients).

General approach to the disclosure of personal information

Paragraph 8 sets out the approach of the common law of confidentiality to disclosures of personal information, and states "You can disclose personal information if:..." before setting out that approach. The approach of the DPA is different here: personal data can be disclosed if it is fair and lawful to do so, and a schedule 2 condition can be identified (and a schedule 3 condition in the case of sensitive personal data, which includes health information) as per the first DPA principle. Whereas for confidentiality the notions of implicit and express consent might be required depending on the purposes for which the information is disclosed, in DPA terms consent
exists either as a schedule 2 condition for non-sensitive personal data, or as explicit consent as a schedule 3 condition for sensitive personal data. For either schedule 2 or 3, if another condition in the relevant schedule can be identified then consent may not be required at all. Whilst of course we do not expect that guidance on confidentiality sets out the DPA approach in detail, the statement "You can disclose personal information if.." might lead doctors to disregard the DPA altogether.

Paragraph 20 highlights another difference between confidentiality and the DPA. It states that "If a patient refuses to consent ... you should ... decide whether the disclosure can be justified in the public interest." From a DPA point of view if consent is sought and subsequently refused then to disclose personal data would be unfair. If it is anticipated that the disclosure has a legal basis to take place anyway, regardless of consent, then for the purposes of the DPA another schedule condition should be applied and consent not sought - patients should simply be clearly informed that the disclosure will take place, to whom and why. The same comment also applies to paragraphs 35 and 37.

Disclosures without consent

As mentioned before this is possible under the DPA if another schedule 2 (and 3 if applicable) condition can be applied. However from a DPA point of view it is important to disclose information fairly, and this requires that patients are clearly made aware that such disclosures will take place. This could be referred to in paragraph 42.

Anonymisation and coding of identifiable information - paragraph 49 If the safe haven or delegate is a separate data controller then this is still a disclosure of personal data and must therefore be carried out in accordance with the DPA. There must be a legal basis for the disclosure and patients must be aware that their data is processed in this way.

9 January 2015