General Medical Council

Regulating doctors
Ensuring good medical practice

GMC response
European Commission stakeholder consultation
Future of data protection
30 July 2010

Introduction

1. The General Medical Council (GMC) is the independent regulator for doctors in the UK. Our purpose is to protect, promote and maintain the health and safety of the public by ensuring proper standards in the practice of medicine.

2. There are currently over 235,230 doctors on the UK Medical Register. 22,020 (9.4%) of these doctors qualified in other parts of the European Economic Area.

3. The law gives the GMC four main functions:

- keeping up-to-date UK registers of qualified doctors
- fostering good medical practice in the UK
- promoting high standards of medical education in the UK
- dealing firmly and fairly with doctors practising in the UK whose fitness to practise is in doubt.

4. The GMC believes the fundamental purpose of medical regulation is to ensure safety and quality of care for patients. That rests on trust between doctors and patients, which in turn relies on patients having confidence that the sensitive personal information they share with their doctors will be treated in confidence and that their privacy will be respected. It also requires the exchange of practitioner data between regulatory and other bodies where this contributes to patient safety.

5. The GMC welcomes the opportunity to comment on the questionnaire circulated in the background paper for the 1 July 2010 stakeholders' meeting. Our response focuses on those issues that are most relevant to medical regulation and patient safety.

6. For more information contact the General Medical Council, 350 Euston Road, London, United Kingdom, NW1 3JN. Tel: +44 161 923 6602. Email: gmc@gmc-uk.org

Question 3. Should the current categories of "sensitive data" be extended to cover (and if so why):

- biometric and genetic data?
- a person's family history?
- minors' data?
- data of a financial nature?
- others (*please specify*)?

7. The Directive refers to 'data concerning health' and the UK Data Protection Act 1998 (DPA) refers to personal information relating to 'his physical or mental health or condition'. Close reading of these terms suggests that 'sensitive data' does not necessarily relate to either biometric and genetic data, or to family history, where they are not influencing or affecting 'health' or a condition. In practice in the UK, however, all information stored in medical records is regarded as 'sensitive personal data' and therefore subject to greater controls. It may be helpful, nonetheless, to avoid any ambiguities or future challenge, to broaden the definition of sensitive data to include biometric and genetic data and a person's family history, or to add a category which might be 'data recorded by a healthcare professional in relation to the provision of healthcare.' This would avoid any future disputes about whether information held in a health record, but not relating to a person's health or condition, should be separately categorised as 'personal data'. In addition, some consideration might be given to the proportionate exercise of subject access rights by family members whose data (in the form of family history and genetic data) is stored in a relative's health record or disclosure by health professionals of such information for the benefit of those family members.

Question 4. Should the personal data of minors be better protected? If yes, how? In that case, should there be a harmonized age limit of 18 years in line with Article 1 of the UN Convention on the Rights of the Child?

8. In relation to health, data about minors is subject to the same protections as data about adults. It would be helpful, however, for the Directive to provide clarity about other rights – for example rights to make a subject access request – and whether this should be age related, or dependant on the child's maturity and capacity to understand. Capacity would seem to be a better guide than age in relation to the exercise of subject access rights, although there appears to be little basis for refusing access to children who lack capacity. It is not clear what harmonisation with the UN Convention on the Rights of the Child is intended to achieve, but any reference to age would be unwelcome if it undermined minors' existing rights to access and control processing of their data, especially in the context of teenage sexual health strategies.

Question 6. How could the "right to be forgotten" be strengthened in view of data retention and the right of deletion, particularly with reference to data protection in the on-line environment? Could the introduction of an autonomous right of the data subject to, for example, explicitly ask for withdrawal of his/her personal data from a website be an effective means of addressing this issue?

9. In healthcare, the right to have records deleted in total (for example when a patient wishes to transfer care to another provider) or to have data deleted from a record that is inaccurate, causes some difficulties. It would be helpful to have a clear guide from the Directive about whether there were circumstances in which a data subject had the right to have data deleted or destroyed, rather than amended or corrected, and how the potentially conflicting rights and interests of data subject and data controller should be resolved in a proportionate manner.

Question 7. Is there a need to strengthen the control of a data subject's own personal data? Could the current data protection legislation be improved by establishing a 'property right' over individuals' personal data ("data ownership")?

10. The question of ownership of medical records is complex and engenders considerable debate in the UK. Ownership of paper or computers in which data is recorded, ownership of data by the data subject, and even ownership of intellectual property by the record maker – particularly if the record includes diagnoses or analysis of some kind all need to be considered and are interlinked. We suggest that there is little to be gained from setting up a new legal framework to accommodate these issues. It is more important to strengthen and clarify data subjects' rights to control the processing of their data, irrespective of to whom the data belongs.

Question 9. Should the current requirement for "unambiguous consent" of the data subject be changed to always require "explicit consent"? If so, how could a requirement for "explicit consent" be implemented and exercised in practice, particularly in the on-line environment?

11. It is important that any distinction that is intended (if any is needed) between the consent required for the use of personal data and of sensitive personal data is more clearly defined, if it is necessary. It may be helpful to consider and distinguish between circumstances in which the data subject takes a positive, relevant action to signify their consent (signing a form; giving a verbal agreement; completing an on-line form or tick box) and those cases where their consent may be inferred because, having been given information about the use of the data, they have not exercised a clearly explained right to object to it being processed for a particular purpose.

Question 13. Should specific safeguards be introduced for the protection of personal data of data subjects with a professional or special official secrecy obligation (e.g. legal profession, medical profession)? If yes, which ones?

12. The background paper to the stakeholders' consultation mentions Article 8 to the Charter of Fundamental Rights. The integration of privacy rights into UK law alongside existing common law principles relating to confidentiality has been the source of some tension and confusion, and there may be benefit in better integration of the right to respect for private and family life within an amended data protection directive. The common law duty of confidentiality, as well as our ethical guidance for doctors, has emphasised the special nature of the relationship between doctors and patients and the centrality of confidentiality to trust in those relationships. The right to privacy is more concerned with the nature of the information, and might better reflect the way in which health services are now often configured, with shared access to electronic health records, for example. The directive might lay out a consistent and explicit approach based on the principle of proportionality both to invasions of privacy and breaches of confidence, taking account of the sensitive nature of health information (see our answer to question 3) and the special obligations of doctors.

13. In the context of our function to maintain a register of doctors and to take action against those doctors whose fitness to practise is in doubt, we believe that the fundamental right to the protection of personal data should not impede measures that allow regulatory authorities from sharing fitness to practise[1] information about healthcare professionals in line with Articles 7 and 13 of Directive 95/46/EC.

14. These provisions are essential in the context of Directive 2005/36/EC which facilitates the mutual recognition of professional qualifications and enables the free movement of doctors and healthcare professionals across the European Economic Area.

15. The GMC supports this free movement. For decades the UK health system has benefited from overseas qualified doctors practising in the UK. However, in an environment where health professionals and patients are encouraged to move across member states a risk to patient safety in one member state is potentially a patient safety risk in another member state.

16. It is essential that doctors and healthcare professionals, exercising their rights of free movement, are only granted registration when they are known to be fit and safe to practise and have no conditions or limitations on the registration and right to exercise the professions. Patient safety and our knowledge of a doctors' fitness to practise relies on other competent authorities sharing the information they hold. If information is not shared efficiently and effectively a doctor could be erased or suspended in one jurisdiction while continuing to practise in another – such a situation is a serious risk to patient safety.

[1] Fitness to practise is the process by which concerns raised about a registered health professional's conduct, competence, physical or mental health, or criminal record, are investigated by a competent authority / regulator. This may lead to a health professional being prevented from practising or restrictions being placed on their practise in order to protect the public.

17. Since 2005, the GMC has coordinated on behalf of all other European healthcare regulators, an informal initiative called Healthcare Professionals Crossing Borders (HPCB) to raise awareness among all healthcare regulators of the importance of effective information exchange between regulatory authorities in the context of Directive 2005/36/EC. HPCB's purpose is to contribute to patient safety in Europe through effective regulatory collaboration in the context of cross-border healthcare and free movement of healthcare professionals. The initiative developed two key voluntary agreements - the Edinburgh and Portugal Agreement - that set out a voluntary approach to regulatory collaboration and information sharing as a contribution to patient safety in Europe.

18. Voluntary approaches provide some improvement however our experience continues to show that the information sharing provisions included in Directive 2005/36/EC are open to varied interpretation based on national approaches to information management and privacy laws. Some regulators, for example, have expressed a desire to exchange information, but are impeded in the extent of that exchange because of national interpretations of data protection legislation. This demonstrates the need for the European Commission to provide clarity as to when regulators should put patient safety ahead of data protection considerations and share information in a collaborative, efficient and transparent way.

19. Several cases of impaired healthcare professionals practising in a European jurisdiction after they have been stripped of their right to practise in another country have come to light and some have been brought to the attention of the European Commission in a number of questions tabled by MEPs in the European Parliament[2].

20. These cases demonstrate that patient safety considerations may sometimes be overlooked as a result of interpretation of personal data protection legislation. They also highlight that it is imperative for competent authorities to be able to disclose, hold, request and act on full and up-to-date information about practitioners, such as simultaneous registrations, dual qualifications and registration and disciplinary history, and make this information available to other regulators. This is in line with Directive 95/46/EC which provides for the processing of data "necessary for the performance of a task carried out in the public interest" (Article 7) and disclosure where there is a public protection requirement (Article 13). It is essential that provisions allowing competent authorities to share fitness to practise information are maintained in any new Commission proposal to ensure that patients and the public have confidence in the healthcare services they receive.

21. The GMC would also welcome further European Commission guidance to assist healthcare professional regulators in exchanging personal data in compliance with their rights and obligations under Directive 95/46/EC.

Question 14. Is there a need for introducing an explicit principle of transparency into the legal framework in order to ensure that data subjects receive adequate and sufficient information about the collection and processing of their personal data and to enable them to make an informed choice? In particular:

[2] Questions: P-3434/09 tabled on 5 May 2009; P-0690-09 tabled on 29 January 2009; H-0350/08 tabled on 28 April 2008; P-1112/10 tabled on 8 March 2010.

a. Should the information to the data subject contain further compulsory elements, such as the competent data protection supervisory authority and its contact details?
b. Should the obligation to efficiently display a "privacy notice" which is conspicuous, clear and intelligible to the average user be introduced?
c. Should a uniform EU-format be introduced to comply with this obligation?

22. A recurring difficulty, especially in the use of health records for research and other secondary purposes, is the lack of information routinely made available to patients about how their records might be used. A clearer duty to provide information may help to improve practice. We are not in a position to comment on the usefulness of suggestions in a or c above, but b would seem to be a positive development.

Question 17. Is there a need to clarify the existing legal framework on the processing of personal data related to health? If so:

a. What are suitable safeguards for the protection of personal data relating to health when processed for 'public health' purposes (e.g., when collected as evidence about the health of the population, outcomes from diseases such as cancer, adverse effects from drugs)?

b. Should there be further safeguards for the protection of personal data relating to health, other than the existing requirement that processing may only take place by a health professional subject to the obligation of professional secrecy?

c. Should there be a specific provision addressing the further use of personal data relating to health (e.g. by third parties for profit-making activities)?

23. The directive might specify that anonymised or coded data should be used for ‘public health’ and other secondary purposes, whenever practicable, in preference to (sensitive) personal data; and that Article 8 rights are not engaged by processing data which is not personal data, e.g. because it has been effectively anonymised. An important safeguard might be found in a requirement to ensure that information about the use of data and data subjects’ rights to object (where appropriate) are widely available and properly promoted.

24. Condition 8(1) in Schedule 3 (Conditions relevant for purposes of the first principle: processing of sensitive personal data) to the UK DPA states that processing may be undertaken for medical purposes by a health professional or ‘a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional’. That allows some welcome flexibility, but it is not clear what an ‘equivalent’ duty of confidentiality is.

Question 25. Should there be a specific provision on the protection of personal data of dead persons?

25. In the UK, data related to the deceased is covered by the common law duty of confidentiality and, to a limited extent, statute law (Access to Health Records Act 1990). There are aspects of the position that are not clear, although the Information Commissioner now gives advice on some common law aspects of the issue. It is not clear to us whether this should be resolved at a national or European level. Any provision to protect the personal data of dead persons should consider the rights and interests of surviving relatives and others with a legitimate interest in accessing the data and in keeping it private, and the diminishing public interest in respecting deceased patients' privacy over time.