

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1. What kinds of personal information do you collect, hold and share? For what purposes do you collect hold and share such personal information?

Comments: The General Medical Council (GMC) is an independent body and we protect, promote and maintain the health and safety of the public by ensuring proper standards in the practice of medicine. Where any doctor fails to meet those standards, we act to protect patients from harm - if necessary, by removing the doctor from the register and removing their right to practise medicine.

Doctors must be registered with the GMC in order to practise in the UK and we collect personal information through the registration process. Some of the information we collect is then published in a list of registered medical practitioners which any person can check to see a doctor's registration status. We also investigate complaints about doctors and publish certain information about our hearings and fitness to practise decisions.

A certain amount of our information sharing activities is facilitated by our express statutory powers under the Medical Act 1983. The Medical Act also gives us a discretionary power to publish or disclose any information about doctors' fitness to practise to any person where we

believe it is in the public interest to do so.

We share additional registration and fitness to practise information with certain groups such as UK health departments, doctors' employers and other regulatory bodies, both UK and overseas. This can be on a routine or ad-hoc basis depending on our statutory duties or the level of public interest.

We have a statutory power to advise doctors on standards of professional conduct and medical ethics. We do this primarily through published guidance, which sets out standards that society and the profession expect doctors to follow throughout their working lives. We have published guidance of relevance on confidentiality, research and children (copies enclosed).

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2. What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.

Comments: Patients need to have confidence that doctors are competent in their field and abide by high ethical standards.

For the GMC, the key benefits of sharing personal information are that accurate and quality information is available to be able to regulate doctors effectively. If information sharing does not take place, there may be insufficient data for patients or employers/contractors to be able to make informed decisions or take appropriate action where necessary.

So far as our guidance for doctors is concerned, we recognise that the key benefit to individuals in sharing personal information about their health is to ensure safe, effective and timely medical care. For the public, the benefits are in public health monitoring and surveillance, clinical audit, advances in medicine through research and in the efficient use of resources, which can be assured and enhanced through the sharing of personal information.

Question 3. What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

Comments: There are data security risks when sharing personal information. Data can be lost in transit, e.g. lost in the post or be at risk of interception during electronic transfer if not encrypted or transmitted on a secure medium.

If we restrict the way any personal information we share can be used, there are risks that the data may ultimately be used in a manner that is incompatible with the purpose for which it was collected depending upon the business practices of the receiving organisation.

The level of intrusion and any impact on individual privacy should be assessed before sharing personal information. For example, the GMC does not disclose a doctor's registered address to all enquirers. When we are under no express legal duty to provide the

information, we assess the public interest and undertake a balance of interest test to help decide if the information should be disclosed.

In our guidance on confidentiality, we explain that the key risk to individuals and the public is that they lose trust in doctors, or in the ability to access confidential health advice or treatment, such that they might be deterred from seeking healthcare or from sharing relevant information honestly with their doctors. Additional risks arise for public health if (even a small minority of) individuals are deterred from seeking appropriate healthcare.

Question 4. What scope and methods of information sharing pose the greatest opportunities or risks?

Comments: There is a significant difference between sharing information we are obliged to make available, those that are facilitated by public interest judgements and those made pursuant to legitimate interests. The more ambiguous conditions for processing personal data under of the Data Protection Act (e.g. Schedule 2 conditions 5 and 6) tend to provide the greatest opportunities or risks when trying to justify information sharing because they can be widely interpreted. To minimise those risks, we set up information sharing protocols and agreements with receiving organisations. Such agreements set out our justification for sharing the information and govern the amount of data to be shared, the format in which it is supplied and any other restrictions of use or access to the information.

We do not set out detailed guidance for doctors about the technical means by which they should share information. That is primarily a responsibility of the health service.

Question 5. Please provide examples of where in your view, public authorities hold too much data or not enough personal information and the reasoning behind your response.

Comments: There are examples of doctors having insufficient information to treat patients safely or effectively when the public authority with which they work does not hold that information in an accessible form. Out-of-hours primary care doctors are the obvious example.

No doubt some patients would regard the level and detail of health information held about them by GPs, hospitals and others to be excessive, particularly where it relates to sensitive issues, such as sexual or mental health, or when it contains information or opinions to which they take exception.

Question 6. Please provide examples of where in your view, private sector organisations hold too much data or not enough personal information and the reasoning behind your response.

Comments:

Question 7. Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial but where it is not currently taking place.

Comments: There may be benefits in much wider and easier sharing of personal information for medical research, financial management or health service planning purposes. These need to be balanced against the risks identified in response to question 3, above. In that nearly all information can be shared with consent, and the importance we attach to privacy rights and duties of confidentiality in our society (and in healthcare in particular), it is not obvious that these benefits would compensate for the risks and harm further sharing (without consent) would entail.

Question 8. Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.

Comments: There are examples of information sharing which is, at best, at the margins of what the law or of what many data subjects would find acceptable, including research projects, such as that undertaken by the Healthcare Commission into diabetes care, whereby general practitioners were asked to provide names and addresses of their diabetic patients to a third party so that the patients might be contacted to take part in a survey. The Patient Information Advisory Group was not asked to consider this project and expressed its concern at the way in which it was undertaken.

We have heard of research uses of DNA information from samples taken by the police (from suspects and victims of crime), where there is little or no suggestion that these uses are explained to subjects, who may have little or no choice in providing samples.

In addition to disclosures between two or more distinct bodies, concerns arise in relation to disclosures within the health service, such as from GPs to primary care organisations (for any number of uses, such as financial audit, target payments) for which the relevant regulations and guidance are at best complex and at worst misleading.

The case between (1) *The Health Protection Agency*, (2) *An NHS Acute Trust and (3) An NHS Primary Care Trust and X and (1) The Secretary of State for Health, (2) The General Medical Council and (3) The Terrence Higgins Trust* [2005] EWHC 2989 (Fam) illustrated how very sensitive personal information is shared between agencies for laudable but ill-defined purposes in an unlawful manner, in this case so as to establish whether further disclosure was appropriate.

Section 3: The legal framework

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

Comments: We think the main strength of the DPA is that it is a reasonably flexible framework that seeks to balance individual rights against public good and the legitimate aims of the organisation. It provides some specific and welcome rights to data subjects to access their data and to control its use in some circumstances. It is, however, written in

impenetrable language, laid out in a manner which makes understanding its implications difficult, even by comparison with other legislation.

One of the Act's weaknesses is that it can be very resource intensive to comply with. For example, the actual cost of complying with a subject access request can be greatly in excess of the flat £10 fee that can be recovered. Another main weakness of the DPA relates to its limitations. It was enacted to implement the European Directive into UK law. It takes little account of the common law, which (in the context of information sharing for purposes of medical research, for example) sets a higher threshold than the DPA (the first principle notwithstanding).

The DPA often uses terminology which is left open to interpretation e.g. terms such as "necessary", "(explicit) consent" and "legitimate interests". This can lead to diverse and possibly conflicting implementations of data protection systems which can impact effective information sharing. These terms can also be interpreted very differently by the data subject. Their perception of what is necessary and not prejudicial to their rights and freedoms may differ greatly from the data controller's, making it particularly difficult to explain the justification for processing.

The 'medical purposes' (interestingly including the management of healthcare services and medical research - absent from the Directive -) condition (8) in Schedule 3 means that most disclosures made by doctors are usually thought to be compliant with the Act, notwithstanding the first principle. The common law sets a much higher threshold, such that considering compatibility with the bulk of the DPA may be effectively pointless, or even confusing.

The confusion and consternation which followed publication of our guidance on disclosures to cancer and other disease registries in 2000 illustrated the potential for misunderstanding. That led to the need for legislation to authorise disclosures for those and similar purposes.

Subsequent legal developments in relation to the common law of confidentiality, particularly around privacy rights under the Human Rights Act, has arguably made understanding the implications of the common law more difficult still.

A revised and expanded DPA might clarify and consolidate into a single Act some of the protections offered by the common law and HRA. We recognise, of course, the challenge this would pose and the flexibility inherent and valued in the common law. The benefits would primarily include clarity and greater confidence on the part of doctors and others who are asked to share information without consent in the public interest. It is probably not realistic to suggest a comprehensive piece (or suite) of privacy legislation, and might not even be desirable (we value the exercise of professional judgement by doctors and other professionals, which is a key element of professionalism), but the current discordance between the DPA and the common law is perhaps too great.

Question 10. In your view how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you think the second principle is? Please provide examples and the reasoning behind your response.

Comments: The second principle overlaps with the first data protection principle to be fair and lawful when processing personal data. If the proposed purpose for processing is incompatible with the original specified purposes it is also highly likely to be unfair and in breach of the first principle.

In the context of disclosures, we may be at risk of breaching the second principle if the receiving party uses the information in a way which is incompatible with our original specified processing, despite attempts to restrict the way the data may be used by contractual methods.

It is difficult to know how well the second principle is adhered to by doctors. It seems clear that in some areas the purposes for which data are obtained are not specified in a manner that the data subject can appreciate. It may be that the purposes are not always entirely clear to doctors except perhaps in the most general way. It is certainly clear that data are processed for purposes that were not specified at the time they were obtained, either because other purposes are subsequently identified or because of a failure on the part of the controller to consider and communicate those uses. An example of the former might be records based medical research, while processing for financial purposes in the health service are a clear and regularly identified example of the latter.

The second principle is important, nonetheless and notwithstanding its overlap with the first principle's fairness requirement, in clarifying in the minds of data controllers the purposes of their processing and to enable communication of the same to data subjects. Such clarity is essential to respect for data subjects' rights and a prerequisite to their meaningful consent (which may be the condition/s relied upon under the DPA or a requirement of the common law).

In the context of healthcare, the primary purpose of data processing will be obvious to patients. Other purposes (such as financial or management planning, research, etc., whether known at the time of collection or decided upon subsequently) might not be so obvious and should be specified. It is clear that not all purposes for which data are processed are made clear to patients; it is important that the law and guidance continues to promote this.

Question 11. What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

Comments: The Information Commissioner's commitment to making data protection simpler has helped to dispel some of the wrongly held beliefs about the Act. However data protection continues to be generally misunderstood and misquoted – in particular as a barrier to information sharing.

Recent high profile personal information losses have put a great emphasis on the importance of data protection. However this may also have affected people's perception of personal privacy. We may see an increase in objections to processing and a reluctance to

consent to information sharing as a consequence of this. To help restore public trust in its effectiveness we suggest highlighting those safeguards in the Act to prevent the misuse of personal information and the Information Commissioner being seen to take effective enforcement action.

In communications from doctors, it is clear that misunderstanding of the DPA, and its interplay with other statute and the common law, is rife. On the one hand, the DPA is regularly, erroneously identified as a barrier to information sharing. On the other, its conditions for processing (in Schedules 2 and 3) other than consent are used to support dubious claims that consent is not required for disclosures, notwithstanding common law requirements, the first principle or other statutory prohibitions.

Question 12. What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA? Please provide examples.

Comments: We responded favourably to the Department for Constitutional Affairs consultation for increasing penalties for deliberate and wilful misuse of personal data and believe there should be tougher sanctions for deliberate, reckless and repeated breaches of the DPA. We support the notion that the Information Commissioner should have greater powers of audit to be able to assess data protection systems and is able to take more robust enforcement action.

While we recognise the plethora of legitimate interests the public and individuals other than a data subject can have in the processing of an individual's data, the safeguard provided by s10 is perhaps unhelpfully and unnecessarily narrow. The development of policy in relation to the National Care Record Service pilots has recently illustrated the high barrier represented by the phrase 'unwarranted substantial damage or distress'. It may be difficult for individuals to convince data controllers or the courts of their distress, in particular. The exceptions provided by s.10(2) suggest that a much broader entitlement to require a cessation of processing (and particularly of disclosure) might be more reasonable. It is worth mentioning, of course, that most individuals are unaware of their s.10 (and other) rights, even when organisations invite them to utilise them by producing standard forms invoking s.10.

Patients complain that it can be very difficult to force amendment of inaccurate information or opinion deriving from the same. When such information is shared or made widely accessible through shared records, their concerns can be heightened.

Question 13. Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.

Comments: Patient safety relies greatly on the effective sharing of information between regulatory authorities across national borders. However, different national interpretations of EC privacy legislation (including of Directive 95/46/EC), and differing organisational and legal conventions means that there is significant inconsistency in the level, frequency and

quality of information that is shared across national borders between regulatory authorities.

We have been at the forefront of EEA action to seek to improve the level of information exchange between European healthcare regulators. However, national data protection and privacy legislation increasingly pose a challenge to effective sharing of information. The GMC has for some time been calling on the European Commission to impose a legal duty on professional healthcare regulators within the EEA to exchange information.

The interplay between the DPA and the common law is a primary cause for confusion in relation to the need for consent for disclosures (for purposes such as medical research). Having more comprehensive primary legislation, incorporating the principles in the Directive, but building upon them and codifying common law protections into statute would be an enormous challenge and would necessarily involve the loss of flexibility in the law, but would provide clarity. In the health setting, professional judgement exercised by individual doctors is a real positive of the current framework; we are aware, however, of the frustrations of others (police, NHS managers, researchers, etc.) in obtaining information in this environment, of criticisms made of individual doctors' decisions and of doctors own sense of uncertainty. That may, however, make for considered and therefore better decisions in individual cases.

The DPA could be clearer on data subjects' rights of access; children's rights in particular can be difficult to comprehend (s.66 supposedly regularised the position in Scotland, but the position in the rest of the UK is less clear, with little apparent foundation for the ICO's assertion that children elsewhere in the UK have the same rights as Scottish children); while the rights of parents when attempting to exercise those rights on behalf of their children (whose competence may be emerging) is a similarly tricky topic. Greater clarity might also be given on the basis on which subject access requests might be refused to avoid causing serious harm to the data subject or to other.

Question 14.

Comments:

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples

Comments: The burdens on organisations that process data do not appear to us to be disproportionate. In fact, the burdens are not nearly as onerous as is sometimes suggested. Data can be processed on the basis of a wide range of conditions and the obligations to data subjects are fairly minimal.

Whilst we have no particular issue with the requirement to notify for a register of data controllers, the notification process itself is presented in data protection jargon and is difficult for non practitioners to understand.

Section 4: Consent and transparency

Question 16. Is it clear whether and when you need individuals' consent to share information about them? Are you clear about the forms that consent should take?

Comments: It is not clear from the Data Protection Act or supplementary guidance when consent is needed to share information or the form that consent should take. For the avoidance of doubt, we tend to use explicit consent to share information for non statutory purposes and where there are no clear public interest grounds. For example, we obtain explicit consent from medical students to process their pre registration information and to share that information with the Department of Health and prospective employers. Explicit consent is the clearest indication that an individual has understood and agreed to the information sharing. Implied consent and opt out options can cause fairness problems later if the individual has not read or understood the data protection notices given.

The first conditions of Schedules 2 and 3 refer respectively to 'consent' and 'explicit consent', which may be slightly confusing; the differences do not appear to play out in practice. In fact, it is not always clear which conditions are being relied upon for any given processing/disclosure and the 'medical purposes' condition (8) of Schedule 3 often makes consent unnecessary for DPA purposes, while consent remains important for compliance with the common law and ethical standards.

It is reasonably clear in the healthcare environment when explicit (or express) consent is required and when implied consent can be relied upon. Difficulties can arise when it is not easy (but not necessarily impracticable or entailing disproportionate effort) to obtain consent, especially in Scotland and Northern Ireland to where the jurisdiction of the Patient Information Advisory Group does not extend. The experiences of the Scottish Secondary Use Service and the efforts of the Northern Ireland Privacy Advisory Committee in producing a Confidentiality Code of Practice might provide insights into attempted solutions to these problems, while the recommendations of the Care Record Development Board's Working Group on the Secondary Uses of Patient Information suggest a reasonable solution for England and Wales. There can be challenges in appreciating the scope of consent given by data subjects. In the use of medical records for research purposes, for example, can it ever be enough to ask a patient to consent to future (undefined in nature or time) research uses of their data? Such consent cannot properly said to be informed. Less extreme examples are obvious and commonplace, where the recollection of data subjects is probably less than accurate and reliance on their consent must be open to question. This problem can be compounded when data subjects are or perceive themselves to be required to acquiesce in order to receive the benefits offered by service collecting their data.

Question 17. What, if any, barriers would a requirement for gaining consent create to the sharing of personal information?

Comments: Sharing personal information on the basis of consent can be difficult for us to administrate. For example, a person may consent to sharing information with one third party but not others.

Consent to disclosure is already a requirement of the common law in most cases. Statute, court orders and the public interest satisfactorily cover most other reasonable bases for

disclosing personal information without consent.

Of course it is not always clear whether a public interest justification is sufficient to dispense with the need for consent: decisions on professional judgement and can only be reviewed retrospectively by the courts (and/or by regulatory bodies). Against this difficulty must be considered the helpful flexibility the existing common law framework permits.

'Tick box' agreements to future (poorly specified) uses of data offend the concept of informed consent.

PIAG approval for medical research related disclosures provide a solution to the common law obstacle when it is difficult to obtain consent, but this should remain a last resort when anonymisation or pseudonymisation is not suitable. It is surprising that there is still no similar solution for Scotland or Northern Ireland. With the development of technological mechanisms for linking pseudonymised records, the need for this (what was originally regarded as an interim) solution may diminish (though it is difficult to imagine its disappearance).

A DPA-style requirement to obtain consent with similar exceptions as exist in the common law might provide clear protections for patients' privacy, enhancing the benefits of an assuredly confidential health service identified above and providing clarity to data controllers without necessarily diminishing the flexibility the common law currently offers.

Question 18. Do you have any suggestions on how to make the sharing of information more transparent?

Comments: It is necessary for doctors and healthcare organisations to use a variety of media to communicate to patients the uses to which their data will be put. These include leaflets and posters, but should include individual communications when practicable and appropriate.

While there is a danger of data subjects being swamped by information of this kind, it is a prerequisite to their understanding the ways in which their data is shared and in empowering them to make decisions about such disclosures.

Question 19. How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability? How valuable is ICO CoP for sharing personal information? How valuable are privacy impact assessments?

Comments: We support the view that privacy impact assessments are a method of good practice to demonstrate that the organisation has considered and addressed risks to personal privacy before implementing new systems. It will become a useful tool to help balance the sharing of information for the public good and safety against the rights of individual privacy.

Section 5: Technology

Question 20. What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

Comments: Technology has made it easier to store large amounts of personal information in one place. However this can increase the risks of data error, loss or unlawful disclosure if appropriate information security measures are not realised and implemented. Also a significant number of people can be affected if a single breach occurs.

The publication of information on the internet has also had an impact on the sharing and protecting of personal information. Search engines and websites make it much easier to discover and data match personal information which has both advantages and disadvantages depending on the circumstances.

For example, when a doctor applies to the GMC for registration and that doctor has previously worked in the United States of America, we can look up their fitness to practise history immediately on the relevant State Board of Medicine's website. Conversely, we do not disclose to general enquirers the existence of complaints about doctors that are closed at an early stage of investigation. Nevertheless a patient may discover the existence of a complaint by searching internet news archives and blogs if it was widely reported on at the time of the event.

So far as the health service is concerned, the National Care Record Service for patient records in England is perhaps the most important technological advance in relation to storage, sharing and protection of patients' medical data in recent times.

The dangers of large scale data storage systems can be (and have been) exaggerated (certainly when compared with existing systems). We are not, however, qualified to comment on the technological aspects of the system.

The experience of similar (smaller scale) experiences in the UK and overseas suggests that patients are not overly concerned by the risks identified in such systems, certainly not to an extent that they have exercised rights to opt-out on any significant scale. We commissioned a literature review of public and professional attitudes to privacy of healthcare data (copy enclosed), one of the conclusions of which was that 'The public appears to be becoming more comfortable with computer technology, which may reduce fears over privacy, but with increasing expectations over security and choice about access to their records.'

Question 21. Should the law mandate specific technical safeguards for protecting personal information?

Comments: Whilst a law mandating specific technical safeguards would greatly assist with addressing data security compliance issues, it may become quickly outdated as technological advances and communication trends are likely to supersede the legislation. An alternative solution could be to insert a statutory duty to publish a code of practice into legislation, similar to the section 46 Code of Practice on the Management of Records under the Freedom of Information Act 2000.

Question 22. How in your view could privacy enhancing techniques such as the anonymisation or pseudoanonymisation of personal information help safeguard personal privacy whilst facilitating activities such as performing medical research?

Comments: In our guidance to doctors regarding research and confidentiality we advise that anonymised (or effectively pseudonymised) data should always be used where this serves the purpose. Otherwise obtaining express consent is the strongly recommended course of action when using identifiable personal data for research.

Anonymisation and pseudonymisation of data provide excellent means of achieving the benefits of medical research while respecting patients' privacy and maintaining the trust of the confidential doctor-patient relationship. Investment in appropriate technology and in the procedures to facilitate the same should be encouraged. The CRDB's Working Group on the Secondary Uses of Patient Information provides a helpful framework for advancing this laudable ambition.

Privacy enhancing techniques can help safeguard personal privacy but there are risks if they are not implemented properly and people may be identified using another source of data. For example, removing names or replacing identifiable information with codes (especially if they include full post codes, NHS numbers, etc.) may not be enough to sufficiently anonymise data for records based research. Attempts to pseudonymise (even if not entirely technically successful) are still better than widespread sharing of names and addresses, though, and should be encouraged along with the separation of e.g. clinical data from personal identifiers which are irrelevant to the purpose.

Section 6: International comparisons

Question 23. Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context?

Comments: In the context of increasing mobility of the medical profession into the UK, from other parts of the European Economic Area (EEA) and across the world, it is necessary for the GMC to seek to obtain information about potential new, or existing, registrants from other regulatory jurisdictions. This information is usually in the form of an individual's registration history and disciplinary information in order that we can have firm assurance that these individuals are safe to practise. There are cases where regulated health professionals, in breach of the prevailing regulatory standards or codes, have sought to move from country-to-country to avoid regulatory action in their home country.

Since 2005 we have led the Europe-wide Healthcare Professionals Crossing Borders (HPCB) initiative that brings together professional healthcare regulators to improve information exchange. The GMC is also a member of the International Association of Regulatory Authorities (IAMRA) and is exploring potential mechanisms for securely and efficiently sharing registration and disciplinary information. The medical profession across the world is highly mobile and in addition to the varying approaches to data protection, differences in regulatory structure and access to information technology can mean exchanging information is also problematic.

In our experience, regulatory bodies in countries such as South Africa, New Zealand, Australia and Canada are receptive to information sharing practices and whilst we have no particular knowledge of their legislative frameworks, these may contain features that could be useful in a UK context.

Question 24. Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

Comments: The State Medical Boards in the United States of America publish more detailed information about a doctor's registration and any formal action taken on the internet. Personal details such as registered and practice addresses are publicly available in order to help identify a doctor. Dates of birth are sometimes available, along with information about where the doctor obtained their primary medical qualification. They also provide more information about any formal action taken – providing a summary of the complaint and action taken and attaching a downloadable copy of the determination. Some Boards cross reference formal action taken in other states so that a patient has a complete overview of the doctor's ability to practise medicine.

The Federation of State Medical Boards (FSMB) in the USA shares information with medical regulators in other jurisdictions. For example, regulators that are able to supply FSMB with the details of registrants on their domestic databases will be notified by the FSMB if it takes disciplinary action against one of those registrants. This helps prevent doctors who have been the subject of disciplinary action in one jurisdiction from simply moving to another jurisdiction where their history is unknown and where they may continue to put patients at risk.

Question 25. Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

Comments: In the European context, there is a great diversity as to the way EC privacy and data exchange legislation has been transposed into national law. Where it is more restrictive than the UK, it can mean that some medical regulatory organisations are less willing to share information about their registrants even when it is a matter of patient safety and public interest.

In our experience, we find Spain's jurisdiction to be particularly restrictive and difficult to work with. They currently do not proactively share information about serious disciplinary sanctions with the GMC. They are also hesitant when supplying information to us on request, even when the information is not particularly sensitive, e.g. when we are seeking to check the authenticity of primary medical qualifications.

Question 26. Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

Comments: The enclosed literature review of public and professional attitudes to privacy of healthcare data was limited to searches of English-language papers only, which restricted materials to the UK, USA, Canada, Australia, and New Zealand, and indexed proceedings of

international conferences. Within these linguistically, legally and culturally similar nations, there was little obvious difference in attitudes.

Section 7: Additional questions

Question 27.

Comments:

Question 28. Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

Comments:

