Chapter 6
Online personal health records
Chapter 6 – Online personal health records

Overview

What is new? Healthcare systems and companies are now using the internet to offer personal online health record systems that individuals can access, edit and share with others. In some cases online health record systems are provided by public and private healthcare organisations (which may set limits as to the type of information that can be added or edited by the patient), and in other cases companies not necessarily involved with the provision of healthcare offer online health record facilities directly to users. The development and use of these records represents a move towards more convenient and patient-centred access to, control of and responsibility for health records, raising issues about responsibilisation and consumerisation in healthcare of the kind discussed in Chapter 2. Indeed, such records can in principle facilitate all of the four types of personalisation identified in Chapter 1.

Which ethical values come into conflict as a result of this development? The principal potential for conflict here is between the value of individuals being able to pursue their own interests in their own way and the value of safeguarding private information. The latter may also conflict with the advancement and maintenance of common good (solidarity), for example over information pooling; and the value of individuals being able to pursue their own interests in their own way may also conflict with the value of activity by the state to reduce harm, for example in the form of loss or misuse of information.

What is the existing pattern of interventions like? Although there is no specific overarching system of interventions for online personal health records, several measures apply that are all of the ‘general governance’ type described in Chapter 4. Like online health information (see Chapter 5), in the UK and many other countries the most significant state-specific legal power relevant to the area of online personal health records is the data protection regime. In addition, commercial companies are bound by fair trading and competition rules, and medical professionals are bound by their professional guidelines and the common law in the way they use individuals’ health records. The advertising standards regime is also relevant to the types of claim that can be made by providers of these services.

What gaps or shortfalls are there in existing interventions? As with online health information, existing interventions by the state or third parties do not make it easy for individuals to assess the quality of the records services being provided to them online. In particular, it is not straightforward for users to find out how their data will be used, stored, passed on or sold to third parties, or what would happen in the case of the company involved going into administration. Existing systems do not actively promote ‘best practice’ in this area, and users cannot easily identify which jurisdiction any particular website might fall under.

What types of intervention might possibly fill those gaps or remedy those shortfalls? Possible interventions span a range of options, including voluntary adoption of good practice, development or greater use of existing systems of redress, third-party accreditation and state regulation introducing required standards. The rapidly changing nature of this domain means that any satisfactory form of intervention needs to be able to keep up with the changes.

What types of intervention do we recommend, and why? Online personal health records have the potential to empower patients and to increase convenience, safety and efficacy. We have found no evidence of any actual harms having been caused, but we see potential risks over the confidentiality and security of health records. We do not wish to prevent people from gaining the benefits of these services, but we want to ensure that users are able to verify that a system is of high-quality and offers suitable safeguards for their personal information. We recommend an accreditation system based on how well information is safeguarded, and we set out what we consider to be best practice over what information should be provided to users contemplating signing up to online health record systems. We also think it is important that companies establish systems to safeguard the confidentiality of the data they hold were they to change ownership or go into administration.
**Introduction**

6.1 Medical records are fundamental to good-quality healthcare. They store and communicate information about a person’s health, conditions and treatments, and that information can be critical to safe and effective treatment (and sometimes for other purposes as well). That is why doctors in the UK registered by the General Medical Council (see Box 4.1) are required to “keep clear, accurate and legible records, reporting the relevant clinical findings, the decisions made, the information given to patients, and any drugs prescribed or other investigation or treatment [and] make records at the same time as the events you are recording or as soon as possible afterwards”.

6.2 Many healthcare systems, including the National Health Service (NHS) in the UK, are moving towards making all their patient records electronic. Electronic records have the potential to enable the sharing of health information more easily and quickly, allowing access to different people and in different locations. The pros and cons of electronic records that allow patient information to be shared among medical professionals have been much debated. We do not explore this issue again here; rather, the focus of this chapter is on the type of online personal health records that can be accessed, created or edited by the person they concern. Such records are provided by both public healthcare systems and commercial companies.

6.3 Online personal health records offered by healthcare providers lend themselves towards more convenient and patient-centred access to, and control of, such information. All types of online health records offer people a chance to be more involved in their own health and healthcare if they value such involvement. Like the growth in online health information (and perhaps more so), the opportunity to manage personal health records online makes it possible that individuals could wish to – or be expected to – take more responsibility for their health and healthcare (see also Paragraphs 2.15–2.17), by being expected to check their medical records. It thus links to the ethical issues posed by consumerisation and responsibilisation discussed in Chapter 2. Although there is little market competition as yet in the UK, it is possible that online personal health records could become an increasingly consumerised product, given that such records can be provided at the users’ convenience, in their own homes, 24 hours a day.

6.4 Use of online personal health records has the potential to at least contribute to all four of the types of personalisation we identified in Chapter 1. As we have said, such records can lend themselves to more consumerised provision and greater individual responsibility, and could also be conducive to more individualised diagnosis and treatment and more ‘whole person’ treatment.

---


203 We note that there are other ways in which patients can access their medical records, such as the routine practice in England of giving pregnant women their maternity notes to keep with them throughout the pregnancy.
Types of personal health record

6.5 Like online health information (see Chapter 5), the different providers of online health records are motivated variously by considerations of public service (such as improving the health of the population, increasing patient access to health records, increasing the efficiency of the public healthcare system), or by commercial interests. And as we shall show below, there are several different types of record systems. The various providers of online health records provide different levels of access for users/patients, ranging from being able only to view the record, to the ability to add information in specified ways that can be identified as originating from the patient, to being the sole creator and custodian of the record, with the possibility of sharing the record with others including health professionals.

‘Tethered’ online personal health records

6.6 What is known as a ‘tethered’ record is one specific to an institution or a healthcare system and usually offers patients the facility to view their own, or parts of their own, medical records online. They may be linked with further opportunities for the user to record other more general health information, such as their weight, amount of exercise taken or amount of alcohol consumed. One such example is the HealthSpace website operated by the NHS in England. HealthSpace is a free, secure online personal health organiser. It is aimed at helping people to manage their health, store health information and find out about NHS services. In addition, the NHS’s current intention is also that everybody in the future will be able if they wish to have online access through the HealthSpace website to their Summary Care Record (SCR), though the future of this system is not certain at the time of writing. This summary includes details of a person’s allergies, current prescriptions, adverse reactions to medicines, current health problems, and summaries of their care. This summary record is the part of the NHS electronic record that will also be available nationally to healthcare professionals, and the system is currently becoming available across the country after some considerable delay.

Uptake of a HealthSpace account was, however, very low during a small pilot phase, with only 0.12% of those invited to participate completing the process, and the figures have not much changed since (for more detail on extent of use, see Paragraph 6.19). The Department of Health Directorate responsible for managing the English NHS National Programme for Information Technology (IT) told us that the registration process was being made more straightforward (see Appendix 3), and a recent survey suggested that a majority of respondents would consider using it in the future. Funding for a similar scheme in Wales has also recently been announced, the aim of the scheme being to produce a website that will allow patients to check their medical records, order repeat prescriptions and book appointments with their

---


205 See: https://www.healthspace.nhs.uk.

206 The Summary Care Record is one element of the NHS Care Record Service, the other element being the Detailed Record. NHS Connecting for Health (2009) What is the Summary Care Record?, available at: http://www.connectingforhealth.nhs.uk/systemsandservices/scr/intro.


210 A survey of users of the NHS Choices website revealed that the majority of respondents said they would use it at least monthly. See: Greenhalgh T, Stramer K, Bratan T et al. (2010) The Devil’s in the detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes, p165., available at: https://www.ucl.ac.uk/news/scriefullreport.pdf.
general practitioner. In Scotland, a small pilot project offering online access to medical records to patients began in April 2010.

6.7 Other examples of tethered online health records systems are those offered by Kaiser Permanente, a healthcare provider in the USA; Patientsite, developed by the Boston-based Beth Israel Deaconess Medical Center; and My HealtheVet offered by the US Department of Veterans Affairs. Such records are accessible to the patient via the internet with the possibility of the patient adding some information.

‘Untethered’ online personal health records

6.8 In contrast to the ‘tethered’ records discussed in the previous section, ‘untethered’ online personal health records allow individuals to add and organise personal health information, as well as integrate health records from different healthcare providers, and share them with other individuals and institutions at will. Such records do not have to be anchored to any one healthcare institution. Examples of untethered online personal health records available include Google Health and Microsoft HealthVault. Currently, the full functions offered by these two particular systems are available only to residents of the USA or authorised patients of certain participating hospitals as they are designed to integrate with certain healthcare providers in the USA. However, a Microsoft spokesman stated in February 2010 that Microsoft were looking “very seriously” at the possibility of extending its service to the UK.

6.9 Although both Google and Microsoft are commercial companies, they currently offer their online health record service to users for no charge. Their publicity stresses the individual’s control of the data. For example, Google Health states: “You are always in control” and “Your health information belongs to you”, while Microsoft notes that “HealthVault offers you a way to store health information from many sources in one location, so that it’s always organized and available to you online.” Both Google and Microsoft state on their websites that they do not sell or share individuals’ information without their explicit consent (with certain exceptions as set out in their privacy policies). Microsoft states that the information in its HealthVault is “not intended to be a substitute for medical records. Information from HealthVault should not be used by health care providers to make treatment decisions without independent evaluation, and only after being copied into the healthcare provider’s own system.” Google notes that “Google Health does not offer medical advice. Any content accessed through Google Health is for informational purposes only, and is not intended to cover all possible uses, directions,

---

218 For example, Microsoft states that “Except as otherwise described in this statement, personal information you provide on the Site will not be shared outside of Microsoft and its controlled subsidiaries and affiliates without your permission.” Such exceptions include disclosure “if required to do so by law or in the good faith belief that such action is necessary to: a) conform to the edicts of the law or comply with legal process served on Microsoft or the Site; b) protect and defend the rights or property of Microsoft and/or its family of web sites; c) act in urgent circumstances to protect the personal safety of users of Microsoft products or members of the public.” See: http://www.healthvault.com/privacy-policy.aspx. Google operates a similar policy, by noting that “Google only shares personal information with other companies or individuals outside of Google in... limited circumstances”. These circumstances include the consent of the relevant individual, a legal requirement to share such information and providing such information to “subsidiaries, affiliated companies or other trusted businesses or persons” where such parties have agreed to comply with the Google Privacy Policy and any other relevant measures. See: http://www.google.com/intl/en/privacypolicy.html#infosharing.
precautions, drug interactions, or adverse effects. This content should not be used during a medical emergency or for the diagnosis or treatment of any medical condition.\footnote{220}

6.10 In 2009, Microsoft partnered with Walgreens (an online pharmacy in the USA) to create an online portal “through which patients can access and share their personal prescription history”.\footnote{221} Access is provided through the HealthVault service. Users are able to download securely their Walgreens prescription history to a Microsoft HealthVault record.\footnote{222} The aim of combining the services is to allow users to “share a complete profile with other health care providers”.\footnote{223} In this way we can see how the online services we consider in this report are being linked together by providers (see also online health information (Chapter 5) and online purchasing of pharmaceuticals (Chapter 7)).

Benefits and harms

6.11 Some potential advantages and disadvantages of online personal health records were set out in Table 3.1.

Potential advantages

- Secure and useful storage;
- convenience;
- interactive records, e.g. alerts;
- worldwide access;
- benefit from research on pooled data; and
- safeguarding function.

Potential disadvantages

- Misuse of stored information;
- advantages of centralised information may possibly be lost through separate information systems;
- difficulties for healthcare professionals if they have to rely on inaccurate or incomplete records maintained by patients; and
- opportunity for promotion of unnecessary or inappropriate treatments/services.

We further explore some of these advantages and disadvantages below.

Reasons people use online personal health records

6.12 Online personal health records are available via the internet to the individual they concern and anyone they choose to share them with, at any location with internet access and at any time. We have said how such records have the potential to be more ‘consumer-friendly’ than earlier systems. Such records involve the individual patient (or potential patient) accessing, maintaining and sharing the health data contained. It has been argued that providing patients with access to their electronic health records may “improve professional and organizational approaches to health care”.\footnote{224} Such records enable individuals to become more interested and involved in, and responsible for, their own health and healthcare, and have the potential to increase health literacy. Some commentators have suggested that patient involvement in decision making is

\footnote{221}Frederick J (2009) Walgreens, Microsoft partner on new online tools \textit{Drug Store News} 29 June, available at: \url{http://findarticles.com/p/articles/mi_m3374/is_7_31/ai_n32103509/}.
\footnote{222}Walgreens (2010) Walgreens offers pharmacy patients access to secure prescription history through Microsoft HealthVault, available at: \url{http://news.walgreens.com/article_display.cfm?article_id=5255}.
\footnote{223}Ibid.
pivotal to improving quality of care, and “some errors and adverse events in healthcare can be avoided through patient involvement.” For example, patients may spot errors and omissions within their own records more easily than health professionals.

6.13 As we noted in Paragraph 6.10, online health services are starting to be combined by providers to offer integrated services such as online health information combined with online health records and online ordering of pharmaceuticals. This development offers great potential convenience and independence for users, but also leads to the possibility that reliance on these facilities would leave such users vulnerable when a company went bankrupt or changed hands. We return to this issue in our recommendation in Paragraph 6.33.

How information is used

6.14 Like online health information (see Paragraph 5.25), there are certain features of online records relating to the way that personal information is used by the provider or third party that can be advantageous or disadvantageous for individual users, depending on how activities are carried out or perceived. For example, an online record system could use the information that users enter to notify individuals about clinical trials relevant to their conditions or market products to them. Whether users find such information useful or bothersome is likely to depend on several things, including the nature of information offered. Moreover, going beyond the individual user perspective, such records offer the possibility of aggregating information for public health, research and commercial purposes (see also Paragraph 5.26). We deal with how those who sign up for such records should be informed about the uses to be made of the information they enter in our recommendations in Paragraphs 6.27 and 6.33.

Potential harms from using online personal health records

6.15 On the harms side of the equation, increasing access to data through online systems also brings new risks to the privacy and security of health records. Such privacy and security matters: for example, the Markle Foundation argues that “inappropriate access to health information can result in discrimination, social embarrassment, or worse”.

In our consultations we heard about the possibility of doctor-patient confidentiality being breached through family members or other contacts demanding or guessing somebody else’s password. More broadly, personal health information entered and accessed online is commercially valuable. The ease with which electronic files may be transmitted and accessed is a double-edged sword: while this feature increases convenience, it also means that (as with all electronic records of personal information) files can be ‘lost’ or misused as a result of carelessness, fraud or institutional change. As for the latter, if a provider of online health record facilities were to go bankrupt or change hands, it might be difficult for users to guarantee that their data were held securely. A company might even abandon the information it held or the relevant computer equipment. We return to this point in our recommendation in Paragraph 6.33.

6.16 Some commentators have expressed concerns that the validity of information in health records used by healthcare professionals may be compromised by enabling the person they concern to edit those records, even in a controlled way. We are not aware of any proposal at present to allow unfettered and unrecognised patient modification rights to the medical records created.


and maintained by healthcare providers, but any move in that direction would raise major issues of legal liability over adverse events and risk compromising clinical standards. To take an extreme example, if individuals could modify their medical record at any time, and such modifications were not marked as being made by the patient, healthcare professionals might not identify that the record had been edited by a lay person and not a healthcare professional. If healthcare professionals had to rely on online personal health records created and edited by the patient, they would not have access to what a healthcare professional might be expected to record, but only to the information the patient chose to divulge and interpret. There is currently little substantive information published on the attitudes of physicians to the use of online personal health records, though some work has been done on this topic.

6.17 Depending on the level of integration between health services, some diagnoses may be available for the patient concerned to view on their online record prior to a face-to-face meeting with a health professional. For example, when someone has a blood test, the results could be automatically entered on their record before a consultation. Such a practice could be useful in some cases when it speeds up the transmission of information, reduces the time needed in costly face-to-face consultations, or even eliminates the need for such consultations altogether. But some health information, including a diagnosis of a serious condition such as HIV (and what is recognised as ‘serious’ may well differ from one individual patient to another) is inappropriate to communicate remotely without a health professional available to explain and interpret the results and provide further information. The Department of Health officials to whom we spoke told us they had provided for such circumstances by delaying patient access to information about certain serious conditions in the online records to which we referred earlier (see Paragraph 6.6), until after the patient has seen a health professional.

Extent of use

6.18 Currently, patients in the UK and in other countries have a right to access their medical records on request (with certain exceptions) and also to have them amended in some circumstances. Records offered by public healthcare systems (including the NHS in some areas) that can be viewed online, and even modified by patients, can be seen as part of a broader movement towards greater transparency in some aspects of healthcare. But there is currently little systematic data about the characteristics of people who use online personal health records.

6.19 As we noted in Chapter 5, internet use has grown rapidly in recent years (see Paragraph 5.27), and the technology necessary to provide sophisticated services online has been developed and implemented. But the adoption rate of personal health records appears to be low. One study in England, which included 103 individuals and seven focus groups, found most people were not aware of HealthSpace (see Paragraph 6.6), nor were they interested in storing or accessing their medical information via this facility. Indeed, many saw the system as "pointless", "irrelevant" or a security risk, although "a small but important minority" saw potential benefit for those with chronic illness. Uptake of such records has so far been slow, and a story in the media in April 2010 reported that, in early 2010, a total of 752 people out of the 1.2 million in England who had Summary Care Records had opted to use the NHS HealthSpace portal to access their records.

230 We recognise that ‘official’ medical records are not always accurate.
231 For example, the American Medical Association recently performed a survey of physicians in the USA on this topic, although the data had not been published at the time of writing.
6.20 A study published in 2006 indicated that 28% of households in the USA tracked health and medical information at that time; of that number, 94% did so using paper records and 1% used web-based systems. Another study carried out by the Markle Foundation in the USA included a survey of consumer attitudes to online personal health records in 2003. The results were based on an online survey of 1,246 people taken to be broadly representative of the adult population in the US in terms of age, race and education. The survey found that over 40% of respondents kept medical records at home, although only 2% did so using a computer. Seventy one per cent thought having health information online would help clarify doctors’ instructions. Over half thought that such online records would help improve the quality of care. In response to the question “If you kept your medical records online, how comfortable would you feel having the following people access your records only after you have given your explicit permission”, 79% responded that they would feel comfortable having their primary doctor access their records, in comparison to 31% for family and 23% for health insurers. Another US study, in 2007, found that of the 26% of US adults that made use of an electronic medical record (which included those maintained by their doctor), only 1% used a personal health record stored on the internet.

6.21 It has been suggested that “there is a gap between today’s personal health records... and what patients say they want and need”; a gap that includes “cost, concerns that information is not protected or private, inconvenience, design shortcomings, and the inability to share information across organizations”. While it has been argued that such a gap must be bridged before personal health records (PHRs) are widely adopted, it has also been noted that the “impediments to PHR adoption are not limited to [the] technical”, before online personal health records are adopted, “societal, interpersonal, and individual level” barriers – such as poorly defined responsibilities for ensuring information accuracy, the possibility that providers will be uncomfortable sharing power, and low levels of technological literacy (notably in older populations) – must be eliminated also. Methods for changing such ‘non-technical’ conditions are said to include “near term system redesign and revised social marketing of the technology”.

Current system of interventions

6.22 Although there is at present no specific overarching system of interventions for online personal health records, several measures apply that are all of the ‘general governance’ type described in Chapter 4. Like online health information, in the UK and many other countries the most significant state-specific legal power relevant to the area of online personal health records is the data protection regime which was referred to in Chapters 4 and 5 and is further discussed below. In addition, companies are bound by fair trading and competition law, and the conduct of

---


242 Ibid.
medical professionals in using individuals' health records is governed both by professional codes and guidelines and by the law of tort and delict. The advertising standards regime to which we referred in the previous chapter (see Paragraphs 5.41–5.42) is also relevant to the types of claim that can be made by providers of online records services. Other responsibilities and liabilities of the various providers of healthcare and healthcare-related products in the UK were summarised in Box 4.1 in Chapter 4.

6.23 Like the other areas in this report involving services provided via the internet, online personal health records are not necessarily limited to people in any one country or jurisdiction. Providers are ‘footloose’ in the sense that provision does not need to be in any one specific location and providers can thus move around if it is advantageous for them to do so. Even though the storage of personal health data via websites opens up risks of loss in various ways – and the commercial value of data also increases the risks of theft and misuse – the footloose character of the online records industry makes traditional state regulation of the type discussed in Chapter 4 difficult to apply, as we also noted in the previous chapter.

**Data protection**

6.24 The different regulatory frameworks relating to privacy and confidentiality that various countries operate, and the lack of an overarching international policy on the subject, means that the protection afforded to an individual’s data may vary substantially among service providers, depending on where they are based (see also Paragraphs 5.37–5.40). For example, organisations and companies based in the UK and the EU are subject to data protection legislation based on a common EU Directive but the legislation or the means to ensure compliance varies greatly in other countries (see Box 6.1 for information about the system in the USA). Even under the UK’s Data Protection Act, the Information Commissioner’s Office told us that if a company holding online personal health records were to go into administration or change hands, there would be no assurance that the data held would either be available to the people they concern to ensure continuity of access, or be secure. We address these issues in our recommendations in Paragraphs 6.31 and 6.33.

**Box 6.1: Regulation of ownership of personal health data in the USA**

The US Health Insurance Portability and Accountability Act 1996 (HIPAA) regulates ownership of personal health data. It requires federal standards for the transfer and use of electronic health data for healthcare providers, health insurance plans and employers.

However, it might be that HIPAA does not apply to all types of health records. For example, Google claims that the health data entered by users of its Google Health records service are given similar protection as that provided by HIPAA but that the data are not actually covered by that law because “Google does not store data on behalf of health care providers”; rather, the relationship is between the user and Google directly. Indeed, some commentators have suggested that Google might close down the Google Health service should the organisation ever come under the aegis of HIPAA.


244 Fact finding meeting 23 September 2009; see Appendix 3.


246 The Working Party’s joint workshop with the Harvard University Program in Ethics and Health (2009).
Softening the ethical dilemmas

6.25 As we have already argued, online access to records has the potential to be one way of enabling people to become more empowered in relation to their health and healthcare and to increase convenience, safety and efficacy. We think that measures by public healthcare providers to enable people to view their own medical records online is important both for allowing individuals to pursue their own interests in their own way and for the reduction of harms (two of the ethical values we set out in Chapter 3). At present there is no clear evidence of harm from the use of online health records either of the ‘tethered’ or ‘untethered’ type we referred to earlier, and it would therefore not be proportionate to use state powers to prohibit the use of, or restrict access to, such records. Nevertheless, there are a number of potential risks associated with such measures, notably those risks concerning our ethical value of safeguarding private information. To soften or reduce the dilemmas arising from potential conflict between the first value noted in Chapter 3 and the second and third values, we therefore recommend a state-sponsored accreditation system for online health records systems and set out some ways in which providers of such systems could improve their services and address the concerns we have about ensuring that private information is safeguarded. As with our recommendations relating to online health information in the previous chapter (and recognising there is some overlap between the two domains), we hope that such measures will generate a climate in which more providers of health records on the internet follow good practice and more internet users come to expect good practice when deciding which services to use.

Services provided and accreditation

6.26 We have already referred to the benefits to their users that online personal health records can offer. But it is not always easy for potential users to assess the quality of the records services being offered to them. In particular, given our concern for the value of safeguarding private information, we observe that it may not be obvious to users how their data will be used, stored, passed on or sold to third parties, or what would happen if the provider went into administration or changed hands. More transparent information about these factors would help users to make more informed choices about their use of online records systems, and our recommendations here are designed to increase such transparency. We recognise that accreditation schemes for websites are subject to certain limitations (see Paragraph 5.47), and that transparency more generally has its limits as a mode of intervention, as we noted in Chapter 4 (Paragraph 4.5). But we think such measures have some useful part to play in helping people to pursue their own interests in their own way in this case.

6.27 Public healthcare services should develop an accreditation system for online health record providers and promote it appropriately. In the UK the responsibility for developing such a system should fall on the Government Health Departments. We recommend that providers of online personal health record facilities should seek accreditation. Such an accreditation system should include requirements to include the following information prominently in lay language:

- the operator of the services;
- location in which the operator is based;
- how information provided by users will be stored, passed on or sold (see also the recommendation in Paragraph 6.33 below);
- arrangements in place to ensure the security and confidentiality of data and information if the operator went into administration or changed hands;
- the possibility that changes to terms and conditions could be made after initial sign-up and how the user will be informed; and
funding and advertising arrangements. Advertisements should also clearly be distinguishable as such.

**Access to online medical records by patients**

6.28 As we have said, some healthcare providers enable patients to access at least part of their medical records online and this access can benefit patients in various ways. There is a risk, however, that not all types of health information and medical records can be interpreted fully by the person they concern without reference to medical knowledge and the current treatments available. Patients may also have perceptions and beliefs that their doctor would wish to talk to them about on receiving test results, given that what is seen as serious by one person may not seem so to another. We know that some online medical record schemes have features that are aimed at ensuring that test results relating to certain serious conditions cannot be viewed by the patient until a face-to-face consultation with a health professional has taken place. We are also aware of concern among some healthcare professionals (see Paragraph 6.16 above) about the implications for decision making if patients were able to modify their own health records. We think careful design of online medical record systems is required in order to take account of such concerns.

6.29 Enabling patients to add (but not delete or edit) health information to an online medical record held by healthcare providers is a sensible measure, provided information originating from the patient can be identified, and provided the system is designed to help both doctors and patients (such as building in limits to the amount and type of information that can be added, to avoid unnecessary burdens on medical professionals to take time in reading through records to protect themselves against possible malpractice suits) and care for their patients. Medical record systems that allow these additions – as is the case with the systems being introduced by the English NHS at the time of writing – can help both patients and health professionals without compromising subsequent decision making by health professionals.

**Safeguarding private information**

6.30 Online health records offered by the NHS and private companies based in the UK are subject to the same data protection legislation as other types of health records and stores of personal information (see Paragraphs 5.37–40 and 6.24). However, as the House of Commons Health Committee noted in 2007’s *The electronic patient record*: "Increasing access to patient data also brings new challenges for safeguarding patient privacy... There is a difficult balance to be struck between the need to protect privacy and the opportunities for research, between safeguarding individual rights and promoting the public good." Indeed, we suggested in Chapters 1 and 3 that using pooled data in medical research can promote solidarity or the common good, one of our ethical values. Clearly this value comes into conflict here with that of safeguarding private information, and such a conflict applies both to online health records operated by private companies and to public healthcare service records. Providers may wish to share the information and data they hold with third parties (such as research institutions or pharmaceutical companies), and users may not always be readily aware of such information-sharing arrangements. The EU Data Protection Directive (the Directive behind the UK’s Data Protection Act 1998) includes the processing of data about an individual both by an organisation established in an EU Member State as well as by an organisation that makes use of equipment for data processing in an EU Member State, so many of the potential harms of online personal health records should be protected against in the EU, and other countries with similar legislation, by data protection laws, provided such laws are adequately enforced. But it is not

---

clear that providers based outside such jurisdictions are in practice always covered by the 
legislation that applies in the countries where their users are based.

6.31 We recommend that responsible bodies in the EU, such as the Information 
Commissioner’s Office in the UK, take as a premise that EU data protection legislation 
applies to online health records held by people who upload and edit their information in 
the EU.

6.32 As an additional safeguard, we would like to encourage what we see as good practice for the 
process by which individuals join online personal health records systems. We believe that 
routinely providing the kinds of information set out below would help users to assess whether 
their private information was being safeguarded. We also think that providers should routinely 
make it easily possible for their users to store their own local copy as an additional safeguard 
against its loss.

6.33 We recommend that providers of online personal health records should design a joining 
process for new users that includes information about the following, which the user 
should actively view and ‘opt-in’ to:

■ arrangements for data security (the possibility of a change to the administration of the 
company);

■ whether and how their personal information will be used, stored, passed on or sold to 
third parties (and the limits of any anonymisation process that may be applied to such 
information);

■ examples about how personal information could be used, such as whether or not the 
user might receive information/advertising from pharmaceutical companies on the 
basis of the information they have entered;

■ the advisability of the user downloading and storing locally a frequently updated copy 
of their health record as an additional safeguard against its loss; and

■ users’ rights under data protection legislation.

The above information should all be presented in accessible language that lay people 
can understand, and advertisements should clearly be distinguishable as such.

6.34 The providers of online health record facilities should design an easy method for their 
users to back up and print out copies of their record to ensure against its loss.
Future impact

6.35 As we noted in Chapter 5, the use of the internet for health-related purposes is likely to grow as more people gain access to the internet across the world and as people who are young and middle-aged now (social groups more familiar with using the internet) become elderly. Healthcare providers may find their patients increasingly demand access to their records and other services online, and commercial competition may drive further development of this kind. The European Commission recently called the facility for individuals to have their personal health information safely stored within a healthcare system accessible online a “right” and offered support for pilot projects to develop such systems.248 Although use of online health records systems outside those offered by public healthcare systems seems to be very limited at present (certainly in the UK), it would be prudent to make arrangements that provided for increased use of such records were it to occur.

---