This is the pre-print version of the chapter.
The original publication is available at: www.springerlink.com
To see the original version of this chapter go to:
http://link.springer.com/chapter/10.1007/978-3-642-22474-4_12

Citation details:
Duquenoy, Penny, Nermeen Magdi Mekawie and Mark Springett (2012) Patients, Trust and Ethics in Information Privacy in eHealth. *eHealth: Legal, Ethical and Governance Challenges*. Carlisle George, Diane Whitehouse, Penny Duquenoy (Editors). Springer-Verlag Berlin Heidelberg 2013. Pp.275-295.

12. Patients, trust and ethics in information privacy in eHealth

Penny Duquenoy*
School of Engineering and Information Sciences, Middlesex University, The Burroughs, Hendon, London NW4 4BT
Email: p.duquenoy@mdx.ac.uk

Nermeen Magdi
School of Engineering and Information Sciences, Middlesex University, The Burroughs, Hendon, London NW4 4BT
Email: n.magdi@mdx.ac.uk

Mark Springett
School of Engineering and Information Sciences, Middlesex University, The Burroughs, Hendon, London NW4 4BT
Email: m.springett@mdx.ac.uk

Abstract

Using Information and Communication Technologies (ICT) in the health sector (eHealth) is a natural progression for the digital agenda, and is seen as being of benefit to organisations providing healthcare, the patients receiving healthcare, and the development of the ICT industry. With the likelihood of a growing demand for healthcare, particularly from an increasingly elderly population, using ICT to streamline processes and support practitioners makes sense. However, the challenges faced when remodelling a sector that has traditionally operated through direct face-to-face human contact are significant. While the processes of information management and information flow may be improved from an organisational perspective, the people at the heart of eHealth, i.e. the patients, may not be convinced that such a move will be of benefit to them, even though the traditional

* Corresponding author

face-to-face aspects may not be lost. In this chapter, we take the example of the United Kingdom and focus on the patient in the eHealth environment. We take the position that patient trust and confidence in ICT is important, not only for patient 'buy-in' but also to maintain the ethical values that are fundamental to medical practice.

Keywords: autonomy, ethics, confidentiality, informed consent, trust, privacy, professionals, professional responsibility, risk, users.

12.1 Introduction

The World Health Organisation (WHO) notes that: "health is increasingly seen as a driver for – as well as a beneficiary of – ICT development in countries (Dzenowagis, 2005, p.2). In the pursuit of the eHealth agenda, the focus of attention has largely been on the policy, practitioner and technical aspects of health provision. Projects have been initiated at national level (e.g. the National Health Service[1], UK) and research into the technical application of ICT for health has received massive funding. The issues of patient confidentiality (i.e. protection and restriction of patient health information) have been the subject of debate and research papers (see for example Williams, 2011; Anderson et.al., 2009). Such attention given to how eHealth could work, both technically and in terms of healthcare management, are good starting points for a health infrastructure that is anticipated to benefit the organisations providing healthcare, the patients receiving healthcare, and the development of the ICT industry in general. Despite recognition that "a more people-centred approach to development" is needed (Dzenowagis, 2005, p.2) the perspective of the eHealth 'end user'[2] is underrepresented. It is important to bring the general public into the picture as, according to this WHO report: "Where physical and financial capital were once seen as critical constraints, social capital became the factor seen as limiting holistic, integrated development" (Ibid.)[3]

[1] National Health Service (NHS) National Programme for IT (NPfIT).

[2] Usually 'end user' is taken to be the person directly using the ICT system. We are taking the 'end user' to be the patient, as the person at the end of the ICT system for whom healthcare is provided and for whom the eHealth initiatives are aiming to support. That is, the patient is the person who is ultimately affected by the system.

[3] The term social capital describes the institutions, norms, trust, and reciprocity embedded in social relations that contribute to the social community, allowing society to coordinate action[3] (Hobbs, 2000; Hobbs, 2001). In the context of ICT and health provision, social capital refers to the embedded relationships that exist in the institution of health provision (e.g. the National Health Service in the UK) and the need to include trust in order to utilise 'social capital'. Thus, it is important to understand and address the impact of issues such as privacy, trust and risk, and the

The chapter's main aim and its contribution to the perspectives of this book, is to present a patient-centred view of the challenges of eHealth. Our approach is to consider the perceptions of people when faced with technology, and services provided online, and how the underlying issues of privacy, trust and risk play out when the service provided relates to health (as opposed to e.g. online shopping or government services).

12.1.1 Overview and structure

In setting out our arguments, the challenges faced, and the recommendations that can be made, we have elected to use a framework that encompasses healthcare practitioners, information systems and technology practitioners, with patients as the 'end user'. This is intended to emphasise a focus on the patient. In the context of eHealth, there are professionals who have a duty of care to a patient, but they are involved in different professions – one set belongs to the medical profession, the other to an information technology (IT) profession. The first is trained in a culture replete with codes of ethics and best practice; the second may or may not be governed by a code of conduct or have had any training regarding ethics and IT. In the case of health information, the parties that have access to patient information extend beyond the healthcare practitioners directly involved with the patient and their care. In any health organisation setting, the system administrators and technical personnel may also have the possibility of access to patient information. Policies, processes, technology design, and education all play a part in influencing their potential culture of ethical behaviour and understanding.

We begin by looking at the role of privacy and the relationship between privacy, trust and risk online using eCommerce and eGovernment as a precursor to eHealth. We then take the perspective of the patient, as a member of the public. Patients are engaged with eHealth and the potential issues impacting on key ethical principles that might be compromised through a move to a broader eHealth landscape where health information can be shared through online services. Following on from this, we discuss concerns that surround patients and their families as carers, as participants in eHealth initiatives with regard to their competence and understanding of information and the Internet, and the relevance of this to informed consent and confidentiality. The chapter finishes with a brief overview of the support available for patients, and for the professionals (healthcare and information technology) whose job it is to provide the infrastructure for patient care, and makes recommendations to address the concerns that have been raised.

---

interdependencies between them, in order to examine population uptake of ICT historically and uptake of eHealth more recently.

12.2 Perceptions of Privacy, Trust and Risk in Online Services

The concept of privacy is notoriously difficult to define (Savola, 2010). It has been characterised as a right, as in the Universal Declaration of Human Rights[4], and encompasses the notion of personal protection in controlling the spreading of information on individuals, or of others intruding on personal space (Warren and Brandeis, 1890). Privacy therefore implies perceptions of boundaries for personal information which can change according to the nature of the information, and its legitimate use. We do not have the space here to explore the various positions put forward on the topic of privacy, many of which are presented by Allmer (2011). For the purposes of our discussion here on patients and the giving of personal information for healthcare we have adopted the notion of the personal control of information about the self, as captured by Goldberg et.al. (1997, p.105): "Privacy refers to the ability of the individual to protect information about himself". Therefore, to the extent that the individual's ability is limited, or even uncertain, we would conclude that an individual's privacy is less assured. This is borne out by measures taken by governments, for example in data protection legislation, and online services that provide reassurances through privacy policies and 'trust' symbols[5].

This section examines perceptions of privacy and how trust influences the choices of people in their online transactions. We follow a timeline from the early days of eCommerce, the development of eGovernment, and finally eHealth. During this period of Internet development, the consumer public has gained more knowledge about the Internet, but at the same time the opportunities for abuse and misuse of information have increased – as has media coverage of these events. Consequently, people have become more aware that personal information provided to online services can be at risk. These aspects of how personal knowledge can be obtained, both on how interactions take place in technical terms and on the threats from abuse and misuse, have a bearing on how people frame the issue of privacy as being relevant to them.

12.2.1 Privacy, Trust and Risk

The definition of privacy provided by Goldberg and colleagues (1997) carries the implication that individuals make an assessment of their ability to protect their information in order to determine what level of protection of their data is possible. That is, they assess whether, under given circumstances, the information someone gives to another is, as it were, safe in their hands. At the heart of this type of as-

[4] Article 12, Universal Declaration of Human Rights, available at: http://www.un.org/en/documents/udhr/ accessed 20/08/2011.

[5] For example, Verisign: www.verisign.com; and TRUSTe: http://www.truste.com

sessment are measures of trust and risk, which go hand in hand. Trust plays a crucial role in consumers' perception of risk; whether it is trust in a person or organisation, or trust in the technology to keep the information secure (Hoffman et.al., 1999; European Commission, 2010). Institution-based trust is also noted by McKnight et.al. (2002) as one of a collection of trust concepts based on attitudes: "disposition to trust, institution-based trust, trusting beliefs, and trusting intentions". In addressing privacy requirements at the technical level, Savola (2010) links privacy and risk in a proposed methodology. Raab (1998) discusses the interplay between trust and privacy in respect of technology and the provision of services, noting that 'virtual transactions' remove familiar trust mechanisms. In respect of electronic commerce (eCommerce), he states that:

"the promise of multimedia convergence may depend upon levels of trust that are needed to sustain electronic commerce, including payments systems. The European Union as well as national governments and businesses have therefore given attention to issues of the security and privacy of the Internet in the hope of gaining public trust for these potentially highly lucrative activities" (Raab, 1998)

Moving from eCommerce to eGovernment the relationship between provider and user are different, since the provision of services changes from the business-customer model to a government-citizen model. Here the issues of risk and trust change shape also. For people using eGovernment services, their choice of provider is limited. An individual may feel more confident that personal information will be used within the limits of the law in eGovernment services (compared to levels of confidence in purchasing goods online). However, there remains a challenge to confidence in the data handling that occurs by staff and the technical measures taken to safeguard personal information. For people to feel confident and use eGovernment they must be reassured about the systems' security and privacy (Sullivan and Clarke, 2010; Abdel-Ghaffar, 2008) as well as trust in the government and the technology (European Commission, 2010). In 2008, following a series of data losses in the UK that were widely reported in the media, a survey on data guardianship was undertaken by the British Computer Society[6]. In answer to the question: "How would you describe your level of trust in established institutions, such as Government departments, to correctly manage your data in the light of recent stories about data breaches or data being lost?" 66% of the respondents said their levels of trust had decreased (BCS, 2008)[7]. These results led to a initiative called "building trust in eGovernment" that focused on "looking at what is necessary to evaluate and manage the benefits against these risks from the citizens' perspective, to ensure that the public sees real net benefit from increased use of technology in government". The working group comprised representatives from expert groups within the BCS including health informatics, security and ethics. As

[6] Officially known as BCS, The Chartered Institute for IT.

[7] The answer options were: increased, decreased, the same, don't know. 1,025 adults aged 16 or over were interviewed.

a result of its work, a Personal Data Guardianship Code was produced (BCS, 2010).

The responsibilities of government associated with provision of online services are also different from the commercial setting, and they provide "unique challenges for government organisations" as reported by Cullen and Reilly (2008, p.77): "[Government organisations] are generally monopoly service providers, and many have the responsibility associated with compulsory data collection for the purposes of collecting revenue ... they must service a wide variety of individuals, across all socio-economic and educational levels, and across a diversity of cultures with equity, courtesy, and sensitivity."

Thus we see that not only are people restricted by choice of service provider in the case of government but also that, conversely, governments have to accommodate all citizens. Although people do not have a choice among organisations when it comes to government services, they do have a choice – at least at present – between the use of online and traditional methods of interaction (e.g. face-to-face, telephone).

If one of the success criteria of eHealth is user acceptance (according to the WHO 2000 report), then attention to perceptions of the users of eHealth on risk, including its benefits and trade-offs, must be addressed. The benefits and trade-offs with eHealth are different again. In order to take advantage of essential and timely healthcare provision, patients need to provide accurate personal and, for some, highly sensitive information (for example, HIV[8], substance abuse, mental illness). The potential impact on the patient if this information were to be mislaid or stolen is arguably higher than if, for instance, credit card details were stolen. Therefore, it is not only vital that patients' information is protected from unintended third-party use, it is also important that patients perceive that to be the case.

A recent study on the views of 490 patients and their physicians (46 in total) undertaken in Canada regarding health information and privacy (Perera et.al. 2011), found that although 48% of the patients and 63% of physicians thought that patient information should be confined to the family physician, more than 90% endorsed the usefulness of computers to facilitate the sharing of health information with other healthcare staff. When asked specifically about computer storage of health information, 40% of patients and 23% of physicians agreed that computer storage of health information would 'make it hard to keep the information private'. Furthermore, half the participants were more concerned about the security of their information if it was transmitted over the Internet.

[8] Human immunodeficiency virus

This overview provides only a snapshot of view on privacy, trust and risk. However, the attention given by online organisations to factors of trust and risk, including privacy, today and the cost of providing such reassurances to their users, is evidence that how users perceive that the privacy of their information online has a significant impact on user take-up of online services. The issues relevant to the uptake of online services are: (i) reassurance on reduced risk and (ii) familiarity with online services. This aspect of familiarity with computer use is discussed in Section 12.3.3.

12.3 Challenges for eHealth

Privacy is of fundamental importance to eHealth especially as it pertains to the confidentiality of personal health data. Personal information held in digital format is vulnerable to loss and theft even if held locally (i.e. on systems within a restricted local network as might be the case in a general health practice). Vulnerability increases as the scope of the network is increased. This is because of the increased complexity of the technology as well as the increase in people using the system. Both technology and human factors are relevant to security of data and information assurance relating to the integrity of the data.

It is, and has historically been, common practice to take measures to protect the confidentiality of patient data for a number of reasons. Patients' medical conditions are personal to them (i.e. patients may not wish to have their medical status known beyond the healthcare practitioners with whom they interact) and knowledge of patients' medical conditions may have an adverse impact on their lives (family relationships, work and career, insurance coverage, among others). Therefore, in order for the patient/doctor relationship to work effectively it is necessary for the patient to trust that the healthcare system will uphold the long-held principle of confidentiality which is instantiated in the Hippocratic Oath: "Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private." (North, 2002)

If patients do not feel that the information that they give to a doctor is protected, in the sense of "considering all such things to be private", and that their privacy is at risk, they may choose to be more selective about the information they provide to the doctor in the future. This can undermine the patient/doctor relationship and impede diagnosis and appropriate treatment. Thus the healthcare practitioner has a responsibility – on behalf of the patient as well as the broader duty to uphold the standards of the profession – to meet patient expectations regarding the confidentiality of health information.

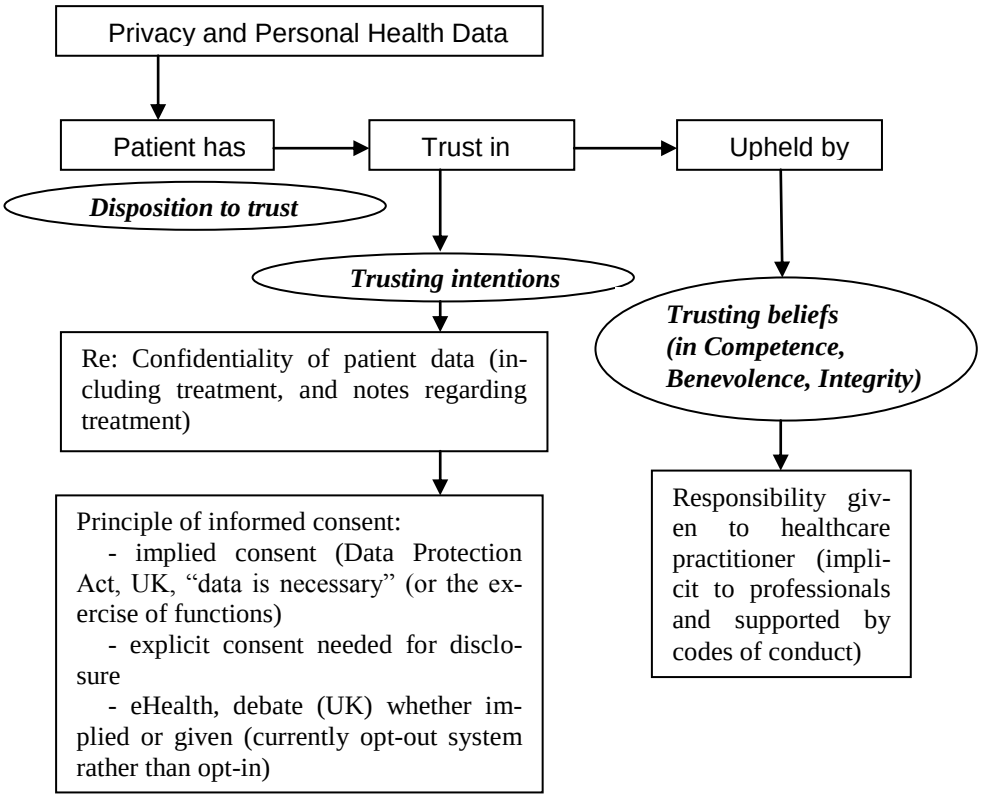
The wealth of research dedicated to the topic of trust in ICT systems development demonstrates the influence of trust on user perceptions and user-uptake of software applications (Kuriyan, 2010). The work in this field is beyond the scope of this chapter. However, in relation to the notion of trust and what it encompasses,

McKnight et.al.'s (2002) categorisation of attitudes regarding trust: "disposition to trust, institution-based trust, trusting beliefs, and trusting intentions" is of considerable use.

The work of Ben-Naim et.al. (2010) also provides an interesting, and relevant, set of characteristics that need to be present to enable trust between a client and a professional. The authors draw on prior work (Barber, 1983; Mayer et. al. 1995) to suggest that the notion of trust encompasses three dimensions: competence (of the person to be trusted); benevolence (attitude of the trusted person to the person seeking trust, including a concern for their interests); and integrity (e.g. to an appropriate set of ethical principles). These three dimensions resonate with the expectations of patients with regard to the patient/doctor relationship. The work describes a framework for making trust judgements relevant to expert systems, and the knowledge that these systems contain.

Taking these ideas together, we can build a picture of privacy in relation to personal health data, trust, and responsibilities indicating the dependence on historic and implicit ethical principles and professionalism. The characteristics of trust outlined by both McKnight and colleagues and Ben-Naim and other authors are inserted in figure 12.1 so as to indicate precisely how they fit with our own concepts (represented by the text in italics).

Figure 12.1: Trust relationships between patient and healthcare practitioner (developed by the authors)



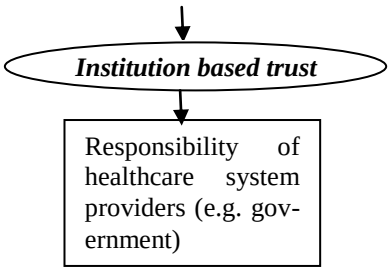


Figure (12.1) above includes an element of trust between the patient and the healthcare practitioner that enables the open communication and expression necessary in the intimate, and life-enhancing or life-diminishing outcome, of healthcare. These foundations of trust – competence, benevolence, and integrity – are implicit in relationships between experts (professionals) and non-experts (clients, or in the case of eHealth, patients). We will discuss in the following section aspects of professionalism and the impact of computer-mediation in the relationship.

In the UK the common law 'duty of confidentiality' applies: "if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent." (Department of Health, 2007, p.2).

"Patients entrust and allow the NHS to gather sensitive information relating to their health and personal matters as part of seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust." [9]

Further elaboration on the duty of confidence from the Department of Health states: "A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence." Further, on patient confidentiality:

. It is a legal obligation that is derived from case law

. It is a requirement established with professional codes of conduct

. It must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

[9] From the UK Department of Health. Online version last modified 19 June 2009. Accessed 18/08/2011

http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084181 Online version last modified 19 June 2009. Accessed 18/08/2011 Online version last modified 19 June 2009. Accessed 18/08/2011

The implications of not meeting patients' trust expectations could have serious consequences, such as:

(i) A reluctance on behalf of the patient to go to a doctor (or other healthcare practitioner) which is likely to have a harmful outcome for the patient (i.e. well-being is reduced), or

(ii) Patients submit themselves to the doctor (or other healthcare practitioner), because they have no other choice available (other than (i) above). This may result in additional stress to the patient and their condition, and have the effect of the patient offering incomplete, or misleading, information about their condition. Both of these outcomes may give an erroneous picture of the patient's status which could lead to misdiagnosis, and possibly inappropriate prescriptions for drugs. As in (i) above, patient well-being could be compromised, in some cases severely.

(iii) A reluctance to use ICT-mediated services (on the part of the patient or the doctor).

(iv) Less patient self-management (in contrast to one of the intended objectives of introducing ICT to healthcare).

(v) Less growth in knowledge and expertise for patients regarding their own health or their health conditions.

(vi) A lower level of compliance with prescribed medications or therapies.

From the point of view of the health service, the impact is a potential loss of trust and confidence in the health system. It could result in the undermining of the system at a broader level, increased workload for healthcare practitioners in trying to overcome the reluctance of information-giving by patients, and increased effort in reinstating reassurance to patients.

12.3.1 Public engagement with ICT for healthcare support

The rhetoric, and research, surrounding the move towards patients' taking control of their health (e.g. European Commission, 2010; NHS, 2010) implies a patient that is 'connected': the patient (or the patient's carer) is in possession of devices that are connected to the Internet or health electronic network in some way. It is not clear what the network technology and infrastructure would be. However, if we take as an example home personal computers (PCs) and mobile phones as tools for information exchange, some challenges arise. There may be a potential lack of understanding by patients as to how their medical and personal information might be communicated between themselves and their healthcare personnel (i.e. doctor, nurse, or other assigned healthcare practitioner) and how, or where, it may be stored.

Principles that are paramount in healthcare practice, such as patient confidentiality, patient informed consent, and the principle of non-maleficence (causing no harm) could be at risk. These challenges arise from the technology as a mediator between the health practitioner and the patient. Various current organisational

practices are relevant in the context of a move towards ICT delivery and provision:

- Doctors, nurses, and other healthcare practitioners undergo extensive training and have an in-depth knowledge of health practices and outcomes, including knowledge of health interventions (such as drugs) and practices (such as cleanliness).
- Records are kept locally and patient information input by medical staff (such as a doctor, nurse, or trained administrative person with an understanding of the medical context and terminology).
- Codes of ethics (according to the area of professional expertise) are embedded in the culture of practice (including the information management relevant to patient confidentiality).

These embedded cultural practices carry with them an understanding of processes and the reasons that underlie the processes. This embedding is at the core of the difficulties that surround the move to patient engagement through ICT:

- When ICT is the mediator, or transmitter of information, the underlying processes are not usually adequately known and understood by the lay person. This lack of understanding could lead to errors in patient data arising at the input stage, or loss of patient information on the system or in transit. For example, if people who use ICT do not understand how information gets from one person, or place, to another they are unlikely to be aware of information security trouble spots or areas of vulnerability. Similarly, the reasons for information management practices are similarly only superficially understood, and may often only be explained in terms of legislation – that is, in countries where that is relevant (in the UK for example the Data Protection Act will apply) – or policies, such as privacy policies.
- ICT professionals working in this field would be expected to have an understanding of data storage and transmission (and the security risks associated with those activities). This may reasonably only apply to particular systems. Where information systems are composed of diverse software applications to achieve different tasks (as is often the case), can it be expected that ICT professionals are sufficiently informed as to either the individual or combined operations of each application? Can this be sufficient to enable the professionals to make an adequate professional judgment on the vulnerabilities, or failures, of information interactions? Furthermore, will the professionals have access to the various parts of the system if a query were to be raised?
- Assuming that medical organisations (such as local medical centres) have such a person on their team or whom they can contact, will they have a deep knowledge or understanding of the particular systems

used by the patients, or the threats to information that might pertain to these individuals (e.g. through access to health records)?

- It has been suggested (NHS, 2010, p.6) that "Giving people control of their care records can also enable them to take greater control of their care". If people were to be given control of their care records some difficulties would need to be addressed. The management of the information in the care record, for example, would require some version control to ensure the information is up-to-date and accurate. Medical terminology and patients understanding of it can also raise challenges for the patient. Similarly patients' own descriptions may not accurately reflect, in the language of the practitioner, the patient's actual health status. However, it appears that in fact people have very little if any control of their care record other than viewing a reduced version online[10]. This in itself raises difficulties for people who do not have online access (including people with physical impairments that prevent them using ICT), or who do not have the skills, competences or physical ability needed to use online services. These people would need to rely on a third party (carer, family member, or friend) to access their care record. People may also be concerned about the security of their care record, as the information on the NHS website informs readers "You must register to use HealthSpace to keep it as secure as possible" and further "No matter how careful we are, there are always risks when information is held on computers, as there are with paper records."
- Complications can arise where some information on the record are considered by the doctor to be harmful to the patient, or detrimental to others[11]. In these case there must be strong security measures in

[10] According to information provided by the UK NHS (www.nhscarerecords.nhs.uk/about) there are two types of patient record. One is the 'detailed care record' which is held locally, and the summary care record which is held nationally, and which contains patient information relating to "medicines you are taking, allergies you suffer from and any bad reactions to medicines that you have had". The summary care record can be viewed by the patient through a website following a registration procedure. There is no detail given for a situation in which a patient does not have access to the Internet, or does not have the skill or capability (physical, cognitive) to access the website. Patients cannot themselves make changes to the record, but can 'discuss' their wishes with healthcare staff. There is no information given about patient access to the detailed care record. Overall it appears that there patients can have very little control of their care record – either detailed or summary. Following the statement above, this suggests they are therefore not in fact "enabled to take greater control of their care".

[11] See e.g. Access to Health Records Act 1990 (UK Government: www.dh.gov.uk)

place (access control mechanisms restricting access to the record) that take into account not only the technical aspects of security but also the human aspects (e.g. failure to log out of a system, use of portable devices by healthcare practitioners, loss of portable devices or storage devices).

These factors affect the notion of informed consent when applied to patients. In the first list of bullet points the historical context is of a doctor (or similar health-care professional) who is trusted to be competent, and can act as a 'professional' (someone with expertise who acts with the permission of, and on behalf of, the less expert – in this case the patient). Where technology is used to communicate and store information or to provide information (as has been suggested in NHS, 2010), the requirements of consent are likely to be those required in data protection laws (that govern the processing of data) or professional guidelines. Whether the person to whom the information refers (i.e. the patient and their health data) can be said to give 'informed' consent is another matter[12]. The person may understand the reason for his or her data to be held, and stored, and communicated – but how that happens, what the risks might be, and the personal consequences should the data be compromised, may not be made clear. A study in 2002 noted that information sheets (relevant to consent) focus on how the information is to be used rather than who can access it, and that consent was not 'informed' since patients were unaware of the many ways the NHS used information and why people needed access to it. The study also noted that patients were 'reassured' and 'happier' when they understood the reasons (Schickle et.al. 2002). We can assume that, as the methods of information and communication become more complex and inter-related (i.e. using mobile phones or home-based PCs), patient understanding of how information transfer in the UK NHS works is important to retain confidence in the system.

Although patients' control of their electronic care record in the UK is limited to viewing it online, or choosing to opt-out (i.e. refusing permission to have their record available in this way) there are other possibilities for communicating medical data between patient and healthcare practitioner. These include the electronic transfer of diagnostic information, such as the results from monitoring blood sugar levels of patients with for diabetes, via ICT devices held by the patient. In such cases, what are the responsibilities of the patient in relation to the device they are using in terms of its maintenance, or data accuracy, integrity, and security? If the patient or their carer/family member/friend is assigned control, are they also given the skills and understanding needed to take adequate control? If they have control, does this imply responsibility? Do new boundaries regarding responsibilities of care records have to be considered? If so, who will decide what those boundaries

[12] An overview of the UK electronic record system and what it means to patients, consent, permission to view, and who can access information is given by Dr Neil Bhatia, GP (no date of origin given on the webpage). Available at: http://www.nhsdatabase.info/ Accessed 3/8/2011.

and responsibilities are, and to whom they apply, e.g. patients, healthcare practitioners, or ICT professionals?

Some of these questions were raised in the PalCom[13] project funded by the European Commission, and reported on in Enquist and Tollmar (2008). A brief overview of the key elements of the project and some outcomes relevant to this discussion are highlighted.

12.3.1.1. Portable data devices

In the PalCom project, a device called the Memory Stone held information related to the medical condition of a pregnant woman and was in her keeping. As described in the paper by Enquist and Tollmar (2008), the device is similar to what is called a 'memory stick' or 'flash drive'. The idea is that the 'patient' (the expectant mother) is in possession of key facts concerning her state of health, and can add her own information from time to time. Using a participatory design approach, discussions surrounding the use of such a device took place. Some stated concerns were around the ownership of the device and the stored data. For example, what happens if the device is lost or stolen? Who owns the stored data? The professionals were concerned about responsibility regarding integrity of the data. If information put on the device was altered by the 'patient', the professionals could not take responsibility for its validity. On the positive side, the 'patient' liked having the device to hand, and felt reassured that information, including reminders of discussions held with professionals, was accessible when needed. However, there were also concerns that, although the information on the device was a duplicate of selected data, information may be lost or degraded. To overcome this issue it was felt that the information storage, although connected, should be separate systems. The safety of the data should the device be lost or stolen was also a cause for concern, and measures to ensure security (e.g. encryption, passwords) were discussed. In this respect, access control was considered important: data should be visible to healthcare practitioners, but not family and friends (for example when the information from the device is displayed on a home personal computer or on a mobile phone) – and vice versa. It was also thought to be significant that the information flow should be apparent to the 'patient' so that it would be possible to detect errors in the information flow.

Hence, the boundaries of responsibility are not straightforward, and maintaining the integrity of the data and ensuring security in case of loss, as well as confidentiality of data, require technical solutions. We can also infer that some level of technical competence and understanding on the part of the patient is required. No discussion by the participants is reported in the paper about technical support for the user, or levels of technical competence. However, the concept of Palpable Computing on which the research was founded incorporates the notion of "putting

[13] PalCom project funded under the EU 6th Framework Programme (IST 002057).

the user in charge"[14] by offering the user information about breakdowns, failures and tools "on how to find out what went wrong and how to correct the error". This suggests that the technical developers are aware of user-control issues.

12.3.2 Patients and technology competence

One area of concern when it comes to patients' perceptions, and management, of privacy is their limited understanding of key technical and organisational issues pertinent to eHealth. This observation can apply to patients of all ages, but it is most likely to be prevalent in older people who have not had the same level of experience with technology that younger people have had. It would also apply to people who have some kind of cognitive difficulty. If one of the objectives of eHealth is to support an increasingly elderly population, the consequences could therefore be serious. Lack of familiarity with the technology could, at the very least, put undue stress on people who are already vulnerable and in need of support. At worst, the system could fail them either technically or as a consequence of their innocence regarding privacy[15]. It may be that elderly patients need a carer or family member to help – which will impact on confidentiality and may cause additional stress. Of course, even without technology mediating healthcare there are many vulnerable people who already rely on third parties to act on their behalf. It may be that, for some elderly patients, technology could provide an accessible solution whereas for others it could further complicate their care.

Patients will increasingly be under pressure to make key decisions about privacy-related issues in relation to the development and delivery of potentially useful eHealth utilities. This lack of understanding and knowledge is something that affects attitudes and decision-making and could potentially lead to more than one possible outcome. It is possible that there will be a level of resistance to involvement in eHealth due perhaps to fears about loss of privacy or the perceived inability of authorities to protect privacy. In other sectors, particularly eCommerce and eGovernment, the issue of privacy has prompted greater efforts to reassure the public so that the potential benefits of the Internet may be more fully exploited. Privacy policies cited on websites as well as standard trust marks are indicators of these efforts.

At a societal level, any resistance by patients to adopt eHealth could lead to degrees of political resistance or, in individual cases, the failure to embrace an optimal technology-assisted utility. Alternatively, a lack of awareness about the range of ethical and organisational issues surrounding the transfer to electronic and online health provision could result in the acceptance of technology change and

---

[14] See http://www.ist-palcom.org/what-is-palpable-computing/ Accessed 18/08/1011

[15] Such innocence regarding privacy is not necessarily restricted to elderly people.

developments that may run counter to the values and material interests of individuals and societies.

Levels of computer literacy vary from country to country, but overall it is only a small minority of populations who have a comprehensive working knowledge of computing concepts such as networking, encryption or spyware. With regard to the privacy and confidentiality of health information, this becomes important if people are asked to give consent to their care record being available on-line or shared with healthcare authorities across the country or other countries. It is unlikely that most people understand where their data is stored (for example if it is 'in the cloud'); or that data losses can occur through such human failings as forgetfulness – mobile phones, memory sticks, and laptops can be easily lost or stolen[16].

There can also be a naivety around levels of privacy and how to manage individual privacy online. For example, users of social networks may be surprised, or even dismayed, when they realise that what they believe to be their private information can be visible to more than just their nominated 'friends'. Similarly, users who respond to emails that promise money or which lead the user to a fake web site may find their personal details used for financial fraud. These are examples of more commonly known email scams which have been in operation for some time. At the technical level and behind the user interface (that is, not visible to users unless they specifically search their computer) the legitimate use of technologies by commercial organisations, such as 'cookies' to collect information from users or more recently the use of 'deep packet' mining exists (collecting information on websites visited in order to provide consumers with targeted advertising). These information-gathering tactics are useful to companies looking to increase sales of goods such as pharmaceuticals (which may possibly be of dubious origin) and to insurance companies looking to build profiles of lifestyle and health status. Technologies such as these, operating behind the scenes, could gather information which the user may prefer to keep private. They can result in unpleasant experiences for users which are likely to affect their attitudes and behaviour online.

12.3.3 Patient empowerment – using ICT for health

Given the situation of diverse technical competencies across populations, how might patients be empowered, technologically speaking, to benefit from eHealth in a knowledgeable and reasonably informed way? How can staff administering eHealth provide support that increases patient autonomy and patient confidence to participate on a more equal level?

[16] Recent reports state that more than 250 laptops have gone missing from the Department of Health (UK) as well as hundreds of BlackBerrys and mobile phones. Computing July 2011.

Growing awareness of the difficulties many people have in using technology is a step forward. In the UK, there are a number of initiatives that have made a start on addressing some of these challenges. Some examples are offered which take the perspectives of: (i) the patient as the user of the health system (ii) the information systems professional, and (iii) the health service professional.

12.3.3.1. The patient as the user of the health system

The issue of privacy and the difficulties experienced by some members of the public regarding technology competence has been recognised for some time. The Information Commissioner's Office (ICO)[17] in the UK provides a number of pages on its website intended to help users, and provides answers to typically relevant questions (such as why and how to manage information, and what to expect from organisations). For members of the public (i.e. a potential healthcare user) easy-to-follow guidance sheets are available[18]. The advice is good, and the lack of knowledge of some members of the general public is recognised by the tone of the leaflet and its generality.

However, to be able to practically understand and follow some of the advice given is likely to need someone with some technical knowledge.
For example, the explanation of what is counted as personal information is very general: "Personal information is information about you. It can be your name, address, or telephone number. It can also be the type of job you do, the things you buy when you are shopping and the place you went to school." A more technical focus features in the advice on buying a home computer: "Buying a good anti-virus, firewall and anti-spam software package will protect your computer against viruses and any spyware software, which can be used to obtain your personal information." Regarding the connection to the Internet the following is offered: "Secure your WiFi. If your WiFi network is not secured, anyone within range can connect to it. An unsecured wireless network is open to hackers to gain access to your personal information. When you buy a wireless router, or if you already have a wireless network installed, make sure you protect yourself by enabling its security features." This latter piece of advice needs some awareness of what WiFi and a wireless network is, including a wireless router, as well as some level of confidence in being able to 'enable its security features'.

Although initiatives such as these are welcome, the level of guidance available in the booklet provided by the ICO does not totally meet the need of the general public. For instance, it is inappropriate in terms of the details needed to understand the risks that might be posed to their health information when they are asked to give consent for the creation of an electronic health record or to benefit from electronic health monitoring initiatives.

[17] http://www.ico.gov.uk

[18] For example the 'personal information toolkit' is entitled: "Advice on how to safeguard your personal information".

12.3.3.2. The information systems professional

For those working within the UK health sector in a technical capacity, the UK Council for Health Informatics Professions[19] promotes professionalism by offering voluntary registration. Its aim is to have all people who spend a substantial proportion of their role or time working health informatics registered with the `council, and therefore "certified as professionals who meet defined standards of professional conduct and competence". Overall, it aims to have health informatics recognised as a profession.

The Council offers knowledge-building support (such as continuing professional development, events, and a library) and a Code of Conduct.

12.3.3.3. The health service professional

The Information Commissioner's Office provides advice on a variety of issues relevant to the Data Protection Act and Freedom of Information Act. This is not specifically aimed at the health service, but aims to support organisations dealing with personal data, In the context of patient data, clear guidance on security is given in "What security measures should I take to protect the personal data I hold?" This guidance document is also relevant to the information systems professional, and is useful for patients in terms of supplying information about security, and the terminology used.

Familiarity with today's technology and privacy issues arising from use of the Internet is not just a matter for patients – as a 2011 publication from the British Medical Association (BMA) indicates. Focusing on professionalism and patient confidentiality the publication "Using Social Media: practical and ethical guidance for doctors and medical students" notes the increasingly blurred boundaries between public and private, i.e. that what is expected to be private is visible to a public (British Medical Association, 2011). In this publication, the BMA draws attention to media reports about employees who have commented on work-related matters, in most cases negatively. The point is made that these social media are often not private, and references made by health professionals to patients – even anonymously – can affect those patients' confidentiality, particularly if a patient could be identified even though not named.

12.4 Conclusions and recommendations

Our starting point in this chapter was that there is a strong push for eHealth, largely by governments, for various reasons including: to provide efficiencies in the healthcare sector, to address the challenge of an increasing elderly population, and to further the digital agenda to contribute to economic growth. This approach is all well and good. However, as with any organisational change, there are chal-

[19] www.ukchip.org

lenges that need to be considered. When healthcare is the focus of change, it is crucial that its longstanding attention to ethics and patient care is maintained.

Throughout this chapter, we have attempted to demonstrate that, for many patients, privacy is perceived to be at risk in the online context. We have argued that a lack of confidence in the maintenance of privacy can have a detrimental impact on people's uptake of online services, and that this will also apply to eHealth. However, because in matters of health there is almost no competition (private healthcare, or 'alternative' therapies excepting), populations will in effect have to 'join in' or 'opt out' of eHealth. In other words, in the eHealth setting the 'customer' does not have the option to choose between more or less trusted organisations (as is the case for online shopping), but is required to use the only method available.

Under these circumstances of little choice, there is a moral obligation for professionals, in healthcare services and information systems, to make every effort to meet the ethical standards expected between a healthcare practitioner and patient. One of the key factors for a good patient/doctor relationship is that of trust. On the patient's side, this involves trust that the doctor will act in the best interests of the patient and, from the doctor's side, trust that patients are transparent with regard to offering details about the precise status of their health condition.

With the well-being of the patient at stake, it is not surprising that healthcare professionals, and health informatics professionals, have put some effort into upholding professional standards as the healthcare sector makes use of developments in ICT. Guidance documents and toolkits have been produced, as well as information on personal data management and data guardianship. There is more to be done that will take time. This will involve embedding information privacy into cultural practice as well as informing all involved of the reasons why privacy is important, including the risks posed by ICT use.

The understanding of risk is not simply the risk of losing information or the impact on the organisation from, for example, reputational loss – as is so often the focus of privacy impact assessments[20]. It is important both to provide reassurance

[20] A Privacy Impact Assessment (PIA) is a self assessment tool used by a certain number of organisations. The UK Information Commissioner's office suggests the objectives of this form of assessment at an executive level are to: ensure effective management of the privacy impacts arising from the project; ensure effective management of the project risks arising from the project's privacy impacts; and avoid expensive re-work and retro-fitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented.
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

to patients regarding privacy of their personal information and have some substance behind the reassurances. If a patient is the focus of a privacy impact assessment then the assessment should assess the potential risk to the patients of information being input, stored, transmitted, and shared, using ICT. Such impacts could be: impact on health care (is the information correct?); impact on identity (from fraudulent appropriation of health information); impact on life opportunities (e.g. information accessed by employers, insurance companies, or through ill-considered use of social networking sites); impact on lifestyle (access to information by family members, friends, and partners).

On the patients' side, support is needed in terms of their understanding of the technologies being used, particularly in terms of their personal information and consent to share that information, as well as support for their use of technology. Many people are still unfamiliar with ICT: this observation refers not just to elderly people but also to others who find the technologies stressful to use. Physical impairments will also have an impact on the ability to use technologies, as will other challenges to access such as cost, literacy, opportunity, and geographic location.

12.4.1 Recommendations

Taking all of the above observations into account, and keeping in mind the efforts undertaken by some UK organisations, we end this chapter by offering the following recommendations:

- Continued training on information governance for all levels of staff in healthcare with an emphasis on the particular characteristics of digital data that cause it to be vulnerable. The data discussed should include not only text, i.e. written health information, but also images related to a person's health status.
- Training and emphasis on data security for those working in technology support – not just encryption, but wider aspects of storage (i.e. data is stored on what, and where – locally, nationally, internationally), logging and tracking of information exchange, and aspects of use (such as policies explaining social media or the use of mobile phones).
- Building on the notion of 'health informatics' professionals as a particular professional category of ICT and providing support for these professionals.
- Incorporating 'user friendly' aspects in the design of devices to be used by patients for their healthcare, and including people representing patients with different levels of ability at the technology design stage.
- Supporting patients in terms of: explanations regarding the technologies used and how they might be affected, technology education, technology provision, opportunities to use non-technical devices (in their own healthcare) without penalty, and options for patients unable to use the technologies.

- Supporting patients by focussing on the issues of trust and privacy of health information to enable measures to be taken at the policy and technical development levels – for example, to develop service models in ways that afford greater control to patients.
- Offering clear guidance throughout the information chain[21] on boundaries of responsibilities that takes into account the range of information flow, including the internet service providers if used.

References List

Journal article

Allmer, T (2011) A critical contribution to theoretical foundations of privacy studies. Journal of Information, Communication & Ethics In Society. Vol 9, No. 2, 2011. Emerald Group Publishing Limited. 2011. ISSN 1477-996X.

Anderson, R. Brown, I. Dowty, T. Inglesant, P. Heath, W. Sasse, A. (2009) Database State. The Joseph Rowntree Reform Trust Ltd. 2009.

Barber, B. (1983) The logic and limits of trust. Rutgers University Press, New Jersey.

Ben-Naim, J Bonnefon, JF, Herzig, A Leblois, S and Lorini E (2010) Computer-mediated trust in self-interested expert recommendations. AI & Society, Vol 25,4, 413-422. Springer-Verlag London Limited, 2010. DOI: 10.1077/s00146-010-0268-4

Bodkin, C. Miaoulis, G. (2007) Ehealth Information Quality and Ethics Issues: An Exploratory Study of Consumer Perceptions. International Journal of Pharmaceutical and Healthcare Marketing 1(1): 27-42.

Cullen, R. Reilly, P. (2007). Information privacy and trust in government: A citizen-based perspective from New Zealand. Journal of Information Technology and Politics, 4(3), 61-80.

Enquist H, Tollmar, K (2008) The Memory Stone – A personal ICT Device in Health Care. NordiCHI 2008: Using Bridges, 18-22 October, Lund, Sweden. ACM 2008.

Goldberg, I. Wagner, D. Brewer, E. "Privacy-Enhancing Technologies for the Internet", IEEE COMPCON'97, pp. 103-109, 1997.

Hobbs, G. (2001) Social Capital Formation in Tanzania. In Selected Studies

[21] The information chain in this context would be from the end-user (patients or their carers/family members), at one end, to the healthcare practitioner or practitioners at the other. It would include the responsibilities of people or companies providing the ICT system and ICT communication link involved in that chain (such as an Internet Service Provider).

of Civil Society in Tanzania: Policy, Social Capital and Networks of the Vulnerable. Waheeda Shariff Samji and Alana Albee (Eds.). UK-DFID, Dar es Salaam, September 2001. ISBN 186192 262 8.
Hoffman, DL Novak TP, Peralta M (1999) Building Consumer Trust Online. Communications of the ACM, Vol.42, No.4, April 1999. pp.80-85.
Ko, Hanjun, Jung J, Kim JY, Shim SW, Cross-Cultural Difference in Perceived Risk of Online Shopping. Journal of Interactive Advertising Vol 4 No 2 Spring 2004. Accessed 24/04/11
Kuriyan, R Kitner, K Watkins, J (2010) ICTs, development and trust: an overview. Information Technology and People, Vol.23. No.3, 2010. pp.216-22. Emerald Group Publishing Limited. DOI: 10.1108/09593841011069130
Mayer, RC Davis JH, Schoorman FD (1995) An integrative model of organizational trust. Acad Manage Rev 20:709-734
McKnight, DH. Choudhury, V. Kacmar, C. (2002) Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research, Vol. 13, No. 3, September 2002, pp. 334-359.
Perera, G Holbrook, A Thabane, L Foster, G Willison DJ (2011) Views on health information sharing and privacy from primary care practices using electronic medical records. International Journal of Medical Informatics. Vol. 80, Issue 2, February 2011. Pp. 90-101.
Samadi, M, Yaghoob-Hejadi, A 2009, A Survey of the Effect of Consumers' Perceived Risk on Purchase Intention in E-Shopping. Business Intelligence Journal, August 2009 p.261-27.
Savola, R.M. 2010 Towards a Risk-Driven Methodology for Privacy Metrics Development. IEEE International Conference on Social Computing/IEEE International Conference on Privacy, Security, Risk and Trust. pp1086-1092. IEEE 2010. DOI 10.1109/SocialCom.2010.161
Schickle, D. Carlisle, J. Wallace, S. Cork, M. Beyleveld, D. Bowns, I.McDonagh, A. Fryers, P. Suckling, R. McCabe, C. Morgan, A. Patient electronic Record: Information and consent (PERIC) - Public attitudes to protection and use of personal health information. 2002. School of Health and Related Research, University of Sheffield. ISBN 1 900752 55 7
http://www.ictri.port.ac.uk/projects1/Patient_Electronic_Record__Information_and_Consent.htm.
Sullivan, K Clarke J 2010 Balancing Security and Privacy in eGovernment Services, Proceedings IST-Africa 2010 Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2010
Sirrka LJ, Todd, PA (1997) Consumer Reactions to Electronic Shopping on the World Wide Web, International Journal of Electronic Commerce, Volume 1, Number 2, Winter 1996-97, pp. 59-88.
Warren, S. Brandeis, L. (1980) The Right to Privacy. Harvard Law Review, Vol. 4. No. 5.

Book
Dzenowagis, J. (2005) Connecting for health: global vision, local insight. Report for the World Summit on the Information Society. World Health Organisation 2005Department of Health (2007) NHS Information Governance: Guidance on Legal and Professional Obligations. 2007
European Commission (2010) A healthy approach – Technology for personalised, preventative healthcare. ICT Research: The policy perspective. Luxembourg: Publications Office of the European Union, 2010. 24 pp. ISBN 978-92-79-16085-1 doi:10.2759/33350
NHS 2010 Liberating the NHS: An Information Revolution. Department of Health, 2010.

Online document (no DOI available)
BCS (2008) BCS Data Guardianship Survey 2008, The British Computer Society. Available online at: http://www.bcs.org/upload/pdf/dgs2008.pdf
Accessed 10/07/2011
BCS (2010) Personal Data Guardianship Code
Available online at: http://www.bcs.org/upload/pdf/pdgc.pdf
Accessed 10/07/2011
British Medical Association 2011 "Using Social Media: practical and ethical guidance for doctors and medical students"
www.bma.org.uk/press_centre/video_social_media/socialmediaguidance2011.jsp Accessed 10/07/2011
Hobbs, G. (2000) What is Social Capital: A Brief Literature Overview. Economic and Social Research Foundation 2000.
http://www.caledonia.org.uk/papers/hobbs.pdf
Accessed 19/08/2011
North, M. 2002 The Hippocratic Oath. National Library of Medicine, History of Medicine Division, United States National Library of Medicine, National Institutes of Health
http://www.nlm.nih.gov/hmd/greek/greek_oath.html
Raab, CD (1998) Trust, Technology and Privacy. Available online at:
http://www.abdn.ac.uk/philosophy/endsandmeans/vol3no1/raab.shtml
Williams, C (2011) NHS 'misleads patients' over sharing medical records with drug firms. The Telegraph, 04 February 2011. http://www.telegraph.co.uk/health/healthnews/8303071/NHS-misleads-patients-over-sharing-medical-records-with-drug-firms.html

Dissertation
Abdelghaffar Ismail HA (2008) Citizens' Readiness for E-government in Developing Countries, Ph.D. Thesis, Middlesex University.

Index