

## **PRIVACY, PATIENTS AND HEALTHCARE WORKERS**

### **A CRITICAL ANALYSIS OF LARGE SCALE, INTEGRATED MANUFACTURING INFORMATION SYSTEMS REAPPLIED IN HEALTH**

**Peter J. Carew and Larry Stapleton**

*ISOL Research Centre, Waterford Institute of Technology, Ireland.*

**Abstract:** This paper examines the social impact of healthcare systems upon two key stakeholders: patients and healthcare workers. The paper focuses upon 'privacy', a growing concern of organisations involved in the delivery of healthcare services. Surprisingly, privacy is typically undervalued in information systems development, including healthcare systems. This paper applies a developmental privacy framework to determine a variety of privacy issues and themes pertinent to the use of ICT for healthcare applications in the context of the two stakeholders above. The paper also notes the absence of human-centred investigations of privacy in healthcare informatics. Finally, the paper demonstrates the usefulness of a recently developed privacy framework in assessing the social impact of advanced technology systems in the healthcare field. *Copyright © 2005 IFAC*

**Keywords:** Medical systems, data privacy, ethics, social impact.

#### **1. INTRODUCTION**

In many societies social welfare systems have developed in response to historical social stability problems. In most western economies access to effective healthcare services is considered to be a major aspect of social welfare and, in Europe, consumes a large proportion of government budgets. It is therefore evident that key technologies associated with the delivery of these systems will have a significant impact upon these societies.

In recent years advanced information technologies originally developed for the manufacturing industry, such as enterprise resource planning systems (ERP), have begun to be installed as healthcare management systems. In this context, these and similar systems gather and process enormous amounts of very sensitive data. Indeed, these systems have received much attention for the problems they have raised in the delivery of healthcare, sometimes leading to fatalities (e.g. Burke and Abramovitz, 2000). This has raised concerns about emerging systemic

problems within health care associated with patient-centredness.

Part of the problem is that these developments have progressed with little in the way of a critical debate within the engineering community as to how these systems impact upon the privacy of individuals. In the context of patient information, this is due, in part, to a lack of any coherent framework by which privacy issues can be debated in the context of advanced technologies.

This paper applies a recently developed and published preliminary privacy framework to health informatics. In doing this it attempts to show how advanced technologies impact privacy issues in the social context. This, in turn, has implications for the stability of social systems which are engaged by such systems. Many of the new technologies, such as ERP, are very ubiquitous, integrating entire national health systems networks. Consequently, these systems impact significantly upon large sections of society and merit deep consideration by researchers concerned with social stability and technology.

## 2. HEALTHCARE, ICT AND PRIVACY

ICT is being increasingly used in medical applications to aid the delivery, efficiency and effectiveness of healthcare. However, ICT use in healthcare applications raises a number of ethical concerns. Privacy is frequently provided as an example of an important and ethically charged issue, but it is frequently undervalued in the ISD and healthcare informatics literature. Palen and Dourish (2003) note that many social and design studies of technology conflate the functions of privacy and subsequently fail to provide appropriate analysis. This paper attempts to help redress this situation and performs a critical analysis of healthcare informatics from a human (or patient) centred privacy perspective.

Patient-centredness involves a complete reorganisation of healthcare delivery whereby the individual patients' problems and needs determine their treatment trajectory (Berg, 2002). However, the term "patient-centred" has become a buzzword and is losing meaning. For example, Berg (2002, p.34) notes, "We preach much more patient-centredness than we practice." Healthcare informatics can only pertain to be patient centred if their use is primarily for the welfare of the patient, not the healthcare organisation. Human-centred design (HCD) is a field of information systems development that places people at the forefront of the development of an information system. In HCD, the needs of people are considered first, then the needs of organisations, and finally the technology required is considered (cf. Brandt and Cernetic, 1998). By applying this tenet of HCD to patient-centred systems design, the patient (human) should be considered first, then the healthcare organisation (hospitals, administration, etc.) and, finally, the technology itself. In principle, a healthcare system cannot be patient-centred if it is not human-centred. Standard development methodologies do not consider privacy as an important human-centric issue (cf. Carew and Stapleton, 2004). Healthcare informatics also seems to have undervalued privacy, treating it largely as equivalent to data integrity, security and availability. Safran (2002) expects that in the future privacy issues will dominate social discourse regarding healthcare informatics, so it is essential that the concept be considered more completely.

## 3. A PRIVACY FRAMEWORK FOR HEALTHCARE INFORMATICS

Privacy is commonly seen as a boundary control process whereby individuals control how much or little contact they have with others at a given time. It can be achieved in a variety of ways, and is very much an individual experience with different individuals having different privacy needs. An optimum level of privacy is generally required by an individual to avoid undesirable behaviour or state of

mind. In short, privacy is an important human-centred value worthy of consideration in the design of any socio-technical system. This paper employs the developmental privacy framework presented in Carew and Stapleton (2004) to identify some privacy issues in healthcare informatics. As the framework incorporates the social and psychological aspects of privacy, the human and patient-centred privacy issues are addressed in some detail. Table 1 summarises the main dimensions of the privacy framework.

**Table 1. Privacy Framework Factors**

Dimension/Id	Factor	Class
Physical		
P1	Environment	T
P2	Territoriality (Property)	T
P3	Territoriality (Body)	T
P4	Solitude (Physical)	T
P5	Repose	T
P6	Physical Access	C
P7	Sensory and Comms Channels	C
P8	Violator (Relationship)	C
Social		
S1	Intimacy (External)	T
S2	Intimacy (Internal)	T
S3	Territoriality (Status)	T
S4	Solitude (Social)	T
S5	Anonymity	T
S6	Autonomy	T
S7	Interactions and Comms	C
S8	Units	C
S9	Formality	C
S10	Personalness of Topic	C
Psychological (Functions)		
Y1	Self-Identity	F
Y2	Personal Growth	F
Y3	Autonomy	F
Y4	Contemplation	F
Y5	Self-Protection	F
Y6	Confiding	F
Y7	Emotional Release	F
Y8	Rejuvenation	F
Y9	Creativity	F
Informational		
I1	Territoriality (Knowledge)	T
I2	Reserve	T
I3	Release of Personal Info	C
I4	Distribution of Personal Info	C
I5	Use of Personal Info	C
Global		
G1	Control	C
G2	Personal Chars and Circumstance	C
G3	Organisational	C
G4	Cultural	C
G5	Societal	C

The framework considers privacy in terms of four main dimensions: physical, social, psychological and informational. The physical dimension refers to the environment (e.g. office, home, hospital, etc.) where an individual may desire physical solitude. Social privacy refers to the freedom individuals have to withdraw from, or enter into, interactions with others. Psychological privacy is closely related to the social dimension, but refers only to the individual psyche. Finally, informational privacy refers to an individual's ability to control personal information.

Many factors related to privacy can be found in the literature and the framework classifies these factors into the four dimensions as appropriate. Each factor is classified as being a privacy: type (T), function (F) or a contributing factor (C). A type is simply a type or state of privacy desired; a function refers to why privacy is sought; and a contributing factor has some influence on the ability to achieve privacy. Some contributing factors have been identified as (mainly) local to one of the four dimensions whereas others have significance across all dimensions. Table 1 provides a list of the privacy factors along with their classifications. Space prohibits a fuller description.

The framework is simply intended to help identify privacy issues pertaining to the development of an information system. For each factor in the framework the main stakeholders' privacy should be questioned in terms of whether the implementation of an information system will affect the factor (i.e. help or hinder an individual's ability to maintain privacy). Those factors identified as potential risks (marked with X in Table 2) can subsequently be addressed. The suitability of this approach is echoed by Hong *et al.* (2004), who propose the use of privacy risk models. These risk models use a (non-prescriptive) list of privacy related questions to identify privacy risks, which are then assessed in terms of a cost-benefit analysis to ascertain and manage those risks which are potentially most damaging. The patient and the healthcare worker (e.g. doctor) are the two main stakeholders with privacy interests related to the use of technology for healthcare. These stakeholders are considered in the following sections.

#### 4. STAKEHOLDER 1: THE PATIENT

For patients the main privacy issues are the change of environment, the changing relationship with the clinician, and the personal information that is collected. The specific needs and concerns of patients are very individual but should be accommodated where at all possible. Table 2 shows the privacy analysis for patients using the framework (columns 4 to 4.4) where potential risk factors are marked with X. The analysis considers the patient in general (column 4) and also identifies some key themes for the patient (columns 4.1 to 4.4). Note that the header for each column identifies the relevant paper section, where the main findings are discussed.

##### 4.1. Patient Safety

Safety benefits offered by ICT in healthcare include: ensuring that correct patient data is recorded, ensuring that appropriate treatment is provided, improved structure and legibility of patient notes, decision support, auditing, and controlled access. Superficially, patient safety would seem to mean that an individual is physically safe while a patient. However, patient safety can be considered well beyond such a definition. Harm can befall an

individual (or their families) as a side effect of healthcare long after the process. Also, harm can be non-physical (e.g. social or psychological). Brennan and Safran (2004, p.548) note, with disapproval, that "the present patient safety initiative focuses on a care horizon that extends only so far as the professionals and health care institutions deem necessary, not to the extent that the patient perceives as relevant. That is, the scope of patient safety rules falls within the scope of the clinical care encounter as determined by professionals." An alternative definition of patient safety would be: an individual suffers no harm (physical or otherwise) as a side effect of undergoing healthcare during or after treatment. Interestingly it is the use of ICT in healthcare, frequently touted as a safety tool, which has allowed for potential patient harm during and after the healthcare process.

Table 2. Results of Privacy Analysis

Fac	4	4.1	4.2	4.3	4.4	5	5.1	5.2	5.3	5.4
P1	X	X				X	X	X		
P2						X	X			
P3	X		X		X		X	X		
P4	X					X		X		X
P5					X	X				
P6	X	X	X			X		X		X
P7	X	X				X		X		
P8	X		X	X	X	X		X		
S1	X	X								
S2	X		X	X		X		X	X	X
S3		X			X	X	X			
S4	X					X		X	X	X
S5	X	X			X	X				
S6	X		X			X	X			X
S7	X		X			X		X	X	X
S8						X	X		X	X
S9	X					X		X	X	
S10	X			X	X					
Y1			X					X	X	X
Y2			X			X			X	X
Y3	X		X			X				X
Y4			X			X			X	
Y4	X	X	X		X	X				
Y6	X	X	X	X		X		X	X	
Y7	X	X	X	X				X	X	
Y8			X							
Y9			X			X				X
I1	X		X			X	X			X
I2	X		X	X	X	X				
I3	X	X	X		X					X
I4	X	X	X	X	X	X	X			X
I5	X	X	X	X	X					X
G1	X	X	X		X	X	X		X	X
G2	X		X		X			X		
G3	X	X		X		X	X		X	X
G4	X	X								
G5	X	X			X					

The danger to patients comes largely from the electronic storing and processing of their data. This data can be accessed by unauthorised individuals (e.g. hackers) and subsequently viewed and changed. Changing record details may result in potentially dangerous treatment being provided, resulting in physical harm. As the healthcare systems store a large quantity of potentially sensitive personal medical information, a given individual may suffer

considerable social harm if third parties obtained certain information. Physical harm may result if the information infers an individual deviates from expected norms (of society or other groups). Even if full information on an individual is unavailable, inferences can be made. For example, being on certain medication can indicate that an individual has a certain illness (e.g. a person on zidovudine will typically be HIV positive (Slack, 2001, p.155)). Psychological harm is very real, and people can suffer psychological harm due to the healthcare process. For healthcare informatics, if sensitive information on an individual were obtained by a third party and subsequently affected a person's life (e.g. social standing, ability to work, etc.) then psychological harm (e.g. stress, depression) could result. Thus, any illegitimate use of information on people can result in people themselves (physical, psychological) or their lives (social) being affected. Existing privacy guidelines and fair information principles (e.g. OECD, 1980) can help distinguish legitimate from illegitimate use.

#### 4.2. Patient Empowerment

Patient empowerment involves informed and knowledgeable patients taking more responsibility for their own healthcare (Grimson and Grimson, 2002). The Internet is pivotal here, with many patients seeking out their own healthcare information (Safran, 2002; Fieschi, 2002). The traditional healthcare model dominated by physicians where patients are simply receivers of health services is giving way to a new model of the self-determining patient/citizen (Stroetmann, *et al.*, 2003). Medical decisions are becoming increasingly collective, involving the patient and an array of healthcare professionals (Fieschi, 2002). Gell (2002, p.71) states "it should be a major goal for the next years to assist patients to retain and exercise as much autonomy as possible in their role as patients." To act autonomously, patients need access to and control over healthcare information stored about them so to control their privacy and make informed decisions.

While patients in principle should be allowed full access to their own records there is a considerable risk of misinterpretation. Therefore, although patients would typically be allowed by law to access all of their EHR (electronic health record) data most patients should only be allowed access to data they can easily interpret and understand (Stroetmann, *et al.*, 2003). Who decides which data patients can safely interpret and access, however, remains an open question that is potentially open to abuse e.g. restricting access unnecessarily. Dreyfus and Dreyfus (1986, p.200) also express concern about patients taking decisions without full information, such as the tacit information that only a doctor's years of experience can provide. Patients will, therefore, still need to trust doctors regarding treatment in some situations.

#### 4.3. Confiding

The opportunity to confide is one major function of privacy (Pedersen, 1997). Reducing the opportunity for one-on-one contact between patient and physician can affect the trust relationship, and this could make confiding more difficult. Whether patients could confide in a clinician via a tele-care service would likely depend on the individual's acceptance of and comfort with such systems, whether they already knew and trusted the clinician, and the nature of the information involved.

#### 4.4. Third Party Use of Patient Data

While the main purpose of documenting care given to a patient is for the continuity of that care, such information is being increasingly used for other purposes such as decision support, quality control, cost control and research (van der Lei, 2002). Access to patient data by third parties is one of the main concerns surrounding the privacy of patient data. Clinicians must have access to a substantial amount of information on a patient to be able to provide safe and effective healthcare. Their need for substantial or full access certainly is legitimate. However, other parties also access patient data but with different agendas. Slack (2001) notes that there are three classes of individuals who access patient data (1) those who have no legitimate reason, (2) those who need part of the patient data to perform their jobs and (3) those who need all the patient data for healthcare. Category 2 is where many privacy problems lie. Some third parties demand patient information beyond that actually required for their purposes. Insurance companies, for example, frequently require full details of patients, tests performed, results, and medical histories. This is clearly superfluous information as all an insurance company should need is some mechanism to confirm that a patient underwent treatment covered by their insurance plan, and an indication of the cost (cf. Slack, 2001). Insurance companies having data beyond this is unethical and a major concern. An obvious danger in insurers having access to patient data is that high-risk cases can be identified and eliminated (i.e. refused insurance). Third parties may have a legitimate need for patient information but, again, this should be limited on a strictly need to know basis (e.g. financial department, researchers). Government agencies do have a legitimate need for access to some data regarding citizens for a greater common good (e.g. to fight terrorism). However, they should not have unrestricted access, and there is widespread distrust towards government agencies respecting the confidentiality of citizen data (Gell, 2002). Overall, third party use of patient data is potentially one of the most privacy-laden topics in healthcare informatics. Again, existing privacy guidelines (e.g. OECD, 1980) can help identify illegitimate third party use. Patients should remain in control of their own information where possible.

## 5. STAKEHOLDER 2: THE HEALTHCARE WORKER

The main privacy issues concerning the healthcare worker are the changing work environment (issues of territory), the changing social space (patients and colleagues), and the amount of autonomy and control enjoyed. Table 2 presents the privacy analysis for the healthcare worker (column 5), again identifying some relevant themes (columns 5.1 to 5.4).

### 5.1. Territoriality

For the healthcare worker, ICT potentially impacts on the property, status and knowledge territories. Property can refer to practically any physical construct and any change to a property perceived to be the healthcare worker's domain can be intrusive. Using ICT in a clinical setting involves changing work practices and procedures, and such changes frequently exclude the healthcare worker from the decision making process (Slack, 2001; van der Lei, 2002). Status is important as it addresses issues of power in the healthcare organisation. Technology is not power neutral and its use can sway power from one set of stakeholders to another (cf. Markus, 1983). For example, technology allows administrators to control the lives of healthcare workers, trace their actions, ensure they follow only standard procedures, and ensure they are working efficiently. Healthcare workers consequently lose much of their autonomy. In terms of knowledge, standardising the recording of data and treatment using ICT restricts the healthcare worker's ability to use other experiential knowledge in treatment, rendering such knowledge less valuable. Denying clinicians the opportunity to use their personal knowledge is potentially intrusive. The fact that healthcare workers frequently have little say in the development of healthcare systems is also problematic, as it ignores the healthcare workers specialised knowledge and expertise. Token healthcare workers may be superficially involved but they frequently have little influence over the final system (Slack, 2001). Thus, the politics under which healthcare workers find themselves should be considered when developing systems (Berg, 2002). People are territorial, and any mishandling (e.g. reducing their status) will create problems.

### 5.2. Sentience and Embodiment

The disembodiment of the patient-doctor contact due to using ICT in healthcare is a major concern. Using tele-care to deliver healthcare or simply using EHR data for diagnoses instead of physically visiting patients contribute to disembodiment. Dreyfus (2001) speaks critically of the lack of embodiment due to tele-presence. He notes that "telepresence can never give us a sense of the reality of far-away things, nor can it convey a sense of trust of distant human beings." (p.98). Dreyfus suggests that when we are not embodied the lack of vulnerability felt

makes the experience seem unreal. Healthcare professionals cannot understand the remote patient's reality due to the lack of context, and may miss implicit signs, which are only available by being physically present with the patient. Dreyfus states that "the body's ability to zero in on what is significant, and then preserve that understanding in our background awareness, enables us to perceive more and more refined situations more and more skilfully; its sensitivity to mood opens up our shared social situation and makes people and things matter to us..." (p.72). This quote strikes noticeable resonance with healthcare, which should be delivered skilfully and in a caring fashion. Disembodiment, thus, makes it difficult to ascertain mood and makes empathy and trust building difficult. Healthcare professionals may feel less vulnerable in treating the "unreal" (or hyper-real) patient and may unknowingly take additional risks. This lack of sentience has been noted in other environments (e.g. industrial). Zuboff (1988), for example, noted that industrial workers used implicit signals to make sense of situations on the factory floor (e.g. noises, vibrations, smells). When automation physically removed the workers from the production processes, they missed the sentience and felt that their problem solving abilities were affected due to this lost information. Healthcare professionals probably also employ a similar sentience in diagnosis and treatment of patients, which would be affected by tele-care systems or relying solely on EHRs for patient information. Tele-care solutions are, thus, not always appropriate. From the patient's perspective, however, some people are comfortable communicating via technology (online support groups, for example, are popular (Safran, 2002)) and may not miss the "human touch" in many situations.

### 5.3. Social Issues

There is a crucial intimacy among healthcare professionals, which facilitates knowledge transfer, motivation and support. Using technology to substitute informal contact with colleagues will effect intimacy and friendship among healthcare workers and could also impact on patient care as informal, personal communications are a preferred way to pass patient information between clinicians (Brown, *et al.*, 2004). Physical social contact is required among healthcare professionals, and this can't be replaced by ICT on assumptions of improved efficiency.

### 5.4. Autonomy

Autonomy used to be a perk of being a doctor (Slack, 2001, p.185). However, healthcare informatics is being used as a tool to standardise care and to make efficient use of healthcare personnel by controlling many aspects of their lives. Thus, doctors no longer have control over their work or treatment of patients. Managers and administrators can trace all of a clinician's actions for accountability and Tayloresque

efficiency purposes. Many information systems have substantial surveillance capabilities, and using technology to monitor healthcare workers clearly affects their autonomy. Superfluous surveillance also suggests a lack of trust, and this can negatively affect the working relationship (Ariss, 2002). The need for accountability and efficiency is being prioritised over the need for flexibility and autonomy on the part of the healthcare worker. This appears to place the needs of an organisation before that of humans, contrary to the philosophy of human-centred design.

## 6. CONCLUSIONS

There are legitimate reasons for recording and processing medical information using highly integrated, distributed systems. However, it cannot be simply treated as another set of data like part numbers, the bill of material or supplier orders. It is inherently sensitive information, and should be afforded special consideration. The potential harm done to patients or society by unintentional and intentional misuse must be considered (Gell, 2002). A full risk analysis must be performed to weight potential harm against potential benefits. Although risks of misuse may be small, this is not a sound basis for deploying potentially harmful technology (Gell, 2002). For healthcare systems to become truly patient-centred they will have to make human factors the top priority and put the care process ahead of peripheral and administrative functions. Privacy is an example of an important human/patient-centred value to consider in this respect, but there is little research that considers privacy from a human-centred standpoint.

In summary, this paper notes that privacy is typically undervalued in information systems development, including healthcare systems. The developmental privacy framework outlined in Carew and Stapleton (2004) is applied to determine a variety of privacy issues and themes pertinent to the use of ICT in healthcare. Finally, the paper notes the absence of human-centred investigations of privacy in healthcare informatics. Ongoing research seeks to redress this issue. Ultimately, the dynamics of social systems will be severely impacted by these kinds of systems. They consequently require more attention by engineers and technologists in order to understand the impact our profession is having upon our society at large.

## REFERENCES

Ariss, S.S. (2002). Computer monitoring: benefits and pitfalls facing management. *Information & Management*, **39**(7), 553-558.

Berg, M. (2002). Patients and professionals in the info. society: what might keep us awake in 2013, *Int. Jour. of Med. Informatics*, **66**(2002), 31-37

Brandt, D. and J. Cernetic (1998). Human-centred approaches to control and info. technology: European experiences. *AI & Society*, **12**, 2-20.

Brennan, P.F. and C. Safran (2004). Patient safety: remember who it's really for, *Int. Journal of Medical Informatics*, **73**(7-8), 547-550

Brown, P.J., S.M. Borowitz and W. Novicoff (2004). Information exchange in the NICU: what sources of patient data do physicians prefer to use?, *Int. Journal of Medical Informatics*, **73**(4), 349-355

Burke, T. and J. Abramovitz (2000). The use of a computer based decision support system in the prevention of adverse drug events, *P & T News*, *May/June*.

Carew, P.J. and L. Stapleton (2004). Towards a privacy framework for information systems development, *Proceedings of the thirteenth international conference on information systems development ISD'2004, Vilnius*.

Dreyfus, H.L. (2001) *On the Internet*, Routledge, NY

Dreyfus, H.L. and S.E. Dreyfus (1986). *Mind Over Machine: The Power of Human Intuition and Expertise in the Era of the Computer*, Free, NY

Fieschi, M. (2002). Info. technology is changing the way society sees health care delivery, *Int. Journal of Medical Informatics*, **66**(2002), 85-93

Gell, G. (2002). Safe, controllable technology?, *Int. Journal of Medical Informatics*, **66**(2002), 69-73

Grimson, J. and W. Grimson (2002). Health care in the information society: evolution or revolution?, *Int. Jour. of Med. Informatics*, **66**(2002), 25-29

Hong, J.I., J.D. Ng, S. Lederer and J.A. Landay (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems, *Proceedings of the 2004 conference on designing interactive systems: processes, practices, methods, and techniques*, 91-100.

Markus, M.L. (1983). Power, Politics and MIS Implementation, *Comms. ACM*, **26**(6), 430-444

OECD (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Palen, L. and P. Dourish (2003). Unpacking "privacy" for a networked world, *Proceedings of the conference on Human factors in computing systems*, Ft. Lauderdale, Florida, 129-136

Pedersen, D.M. (1997). Psychological functions of privacy. *Journ. of Envir. Psych.*, **17**(2), 147-156.

Safran, C. (2002). Commentary - health care in the information society, *International Journal of Medical Informatics*, **66**(2002), 23-24

Slack, W.V. (2001) *Cybermedicine. How Computing Empowers Doctors and Patients for Better Health Care*, Jossey-Bass, CA.

Stroetmann, K.A., M. Pieper and V.N. Stroetmann (2003). Understanding patients: participatory approaches for the user evaluation of vital data presentation, *Proceedings - 2003 conference on universal usability, Vancouver*, 93-97.

van der Lei, J. (2002). Info. and communication technology in healthcare: do we need feedback?, *Int. Jour. of Med. Informatics*, **66**(2002), 75-83

Zuboff, S. (1988) *In the Age of the Smart Machine: The Future of Work and Power*, Basic, NY