

The Concern of Electronic Medical Record about Confidentiality: the Information Professional's Roles and Responsibilities

黃興進^a 洪萬富^b 陳振源

國立中正大學資訊管理研究所^{a b} 南華大學資訊管理研究所

mishgh@ccunix.ccu.edu.tw^a wonder@mis.ccu.edu.tw^b f8721003@yahoo.com.tw

Abstract

Confidentiality is generally important in medicine. Prior research on confidentiality has tended to concentrate on physician patients relationship issues. The roles of information professionals have been generally ignored. Information professionals are increasingly assuming responsibility for planning, building, and running EMR that affect healthcare professionals' operations. The article directly addressed two key questions: (1) What the information professional's roles and responsibilities on the EMR confidentiality? (2) What kind of individual is most suitable for this role? First, in order to realize the importance of confidentiality in EMR, an attempt has been made in this paper to understand the concept of confidentiality, privacy, and security. Secondly, a research framework from the individual-based perspective is developed. Finally, some propositions are developed from literature in the healthcare industry.

Key words: Electronic medical record (EMR), Confidentiality, Information security, Privacy, Individual Ethical Ideology

Introduction

Hospitals improved cost effectiveness based on analyses of electronic medical record (EMR); physicians desire to decision support aids and improve health care through access to EMR; patients need for self care by timely access to EMR; researches need for better research support by EMR. With move to widely accepted EMR, awareness of confidentiality issues has increased among hospitals, physicians, patients, and other healthcare

players in recent years. Confidentiality is a core ethical principle that provides guidance in terms of developing and maintaining a meaningful relationship among healthcare players (Dierks, 1993). Each professional has a primary obligation and take reasonable precautions to respect confidentiality rights in EMR (Barrows and Clayton, 1996).

Confidentiality is generally important in medicine. From the ethical perspective, confidentiality is a way of respecting the dignity of the patient. The patient's most personal physical and psychological secrets are kept confidential in order to decrease a sense of shame and vulnerability. From the pragmatic perspective, if physicians and other professionals are to elicit information from patients, they must be able to guarantee that what is revealed will be confidential. In the absence of such a pledge, there can be no assurance of candor, and in the absence of candor, the capacity to engage in effective clinical work would be impaired (Elliott, 1999). Thus, confidentiality is also an essential prerequisite for the accessibility of the EMR, an important aspect of the right to health. Effective health care requires that patients feel free to come forward to seek medical advice or necessary treatment, and do not feel inhibited from entrusting physicians with information of a personal nature.

Furthermore, The roles of information professionals have been generally ignored on confidentiality concern research. Information professionals are increasingly assuming responsibility for planning, building, and running EMR that affect healthcare professionals'

operations.

Prior research on confidentiality has tended to concentrate on physician patients relationship issues (Gary, 2004). The article directly addressed two key questions: (1) What the information professional's roles and responsibilities on the EMR confidentiality? (2) What kind of individual is most suitable for this role?

First, in order to realize the importance of confidentiality in EMR, an attempt has been made in this paper to understand the concept of confidentiality, privacy, and security. Secondly, a research framework from the individual-based perspective is developed. Finally, some propositions are developed from literature in the healthcare industry.

Confidentiality, Privacy and Security on EMR

Confidentiality is the actual protection action among healthcare player. An individual's personal and health information include those that were supplied by the individual and those observed by the healthcare giver during the course of the delivery of care. Privacy in the

healthcare context amounts to the freedom and ability to share an individual's health information in confidence. Security is the measure that a hospital has employed to protect the confidentiality of the patient information. In essence, privacy of an individual's health information depends on the level of confidentiality maintained by hospitals, which in turn depends on the security measures implemented by them (Krishnamurty et al., 2001). Security measures that are fail-safe must be utilized. Yet, the hospital's security measures can work only within the walls of the hospitals and among its employees. Protection outside the provider requires legislative measures, in addition to hospital's security measures. Therefore, protecting the privacy of patient information is a joint responsibility of hospitals, physicians and patients as a whole; appropriate effort must be put forth by all of them.

There are distinctions between the terms privacy, confidentiality, and information security, and it is appropriate to establish those definitions (Table 1).

Table 1: difference definitions

Articles	Confidentiality	Privacy	Security
Gary Kurtz, 2004	The understanding that medical information will only be disclosed to authorized users at specific times of need.	The right of an individual to control disclosure of his or her medical information	The processes and mechanisms used to control the disclosure of information.
Kim and Choi, 2003	The controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.	The right and desire of a person to control the disclosure of personal health information.	A collection of policies, procedures, and safeguards that help maintain the integrity and availability of information systems and control access to their contents.
NII Advisory Council, 1995	A tool for protecting privacy. Sensitive information is accorded a confidential status that mandates specific controls.	The ability of an individual to control the use and dissemination of information that relates to himself or herself.	Protects both the system and the information contained within it from unauthorized access and misuse, and accidental damage

In summary, concerns over privacy, confidentiality and security will continue to grow as reform measures are implemented, the use of clinical information systems

grow, and the technology for electronic patient records becomes available. It's up to us to help begin laying the

groundwork now to protect both patients and healthcare workers in the future.

Confidentiality concern in EMR

The concern about confidentiality are a significant issue needing to be addressed in any EMR plan. Confidentiality of EMR may be compromised either by patients authorized to access the EMR systems or by unauthorized users. Loss of confidentiality occurs through unauthorized disclosure of information through attacks such as media theft, interception, or misuse by hacking or scavenging. The rapid increase in the amount of data being stored, the number of people who have access to such data, and the ability to perform sophisticated analysis on such data, has focused attention on the topic of inferential disclosure and security (Krishnamurty et al. 2001).

Krishnamurty et al. also classified inferential disclosure into two major categories, namely, identity disclosure and value disclosure. The issue of identity disclosure is of critical importance in situations where the collection of the data is performed with the guarantee of anonymity. In the context of most commercial organizations however, the fact that an individual is a part of the organizational databases does not in itself constitute a breach of confidentiality. By contrast, the disclosure of the value of a confidential attribute for a given entity would constitute a breach of disclosure for both types of organizations (Krishnamurty et al. 2001).

The specification of this pre-specified acceptable level is usually based on the sensitivity of the confidential attribute. The more sensitive the attribute, the lower the acceptable level of accuracy (and higher the security). While it is tempting to specify an extremely high acceptable level of security for all confidential attributes, the presence of non-confidential attributes may make it impossible to achieve these security levels.

In summary, the requirement of providing access to EMR while at the same time protecting confidential numerical values from disclosure, are important issues in a hospital's context. Identity and value disclosure are major issues and deserve immediate attention. The modern society appears to have accepted the "invasion of unauthorized users" necessary for some level of technology. However, the potential misuse of health information at an individual level is a more serious concern. Others counter the loss of confidentiality with the potential harm of a physician treating with incomplete information in emergency or even non-emergency cases because we have overprotected the information.

Fair information practices

The fair information practices which was codified in the 1973 U.S. Department of Health, Education and Welfare report entitled, Records, Computers and the Rights of Citizens. These principles have had a significant impact on the continuing development of a uniform federal privacy policy. The five key principles of fair information practices are: (1) No secret personal data record-keeping systems may exist. (2) Individuals must be able to discover what personal information is recorded and how it is used. (3) Individuals must be able to prevent information about them, obtained for one purpose, from being used or made available for other purposes without their consent. (4) Individuals must be able to correct or amend a record of information about them-selves. (5) An organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.

The conclusions reached by the studies cited above principles that IS professionals are not overtly communicating their willingness and intention to fulfill their duty to protect confidentiality. However, these five

principles define duties at a fairly general level. To understand what the fair information practices mean for IS professionals, it is necessary to examine individual factors.

Individual Ethical Ideology

Many studies investigated which variables can explain practitioners' variant ethical behavior. Personal ethics and age have been repeatedly found to correlate with ethical behavior. However, practitioners with higher standards of personal ethics showed stricter judgment of professional ethics than practitioners with lower standards of personal ethics. Shamir et al. concluded that personal ethical norms with which one entered the profession determined the level of following professional ethics over one's career (Shamir et al., 1990). Forsyth has concentrated on developing a framework through which individuals' ethical orientation can be explained (Forsyth, 1980). He proposed two factors for differentiating the internal ethical orientation among individuals: relativism and idealism. According to this taxonomy using of two factors, an individual may use one of four different methods when making an ethical judgment. High levels of idealism and relativism characterize situationists. A situationist rejects absolute moral rules, and advocates individualistic analysis of each act in each situation. An absolutist has a high level of idealism but a low level of relativism and believes the existence of universal moral rules. The opposite end of absolutism is subjectivism. Subjectivists are usually ethical egoists who make judgments based on personal feelings. Exceptionists who have low levels of both idealism and relativism can be compared to teleology and easily described as utilitarian. Forsyth's taxonomy has been used to identify the influence of individual ethical ideology on ethical attitude, behavior and judgment in various contexts. Applying Forsyth's taxonomy to public relations ethics, this study predicts that practitioners with different kinds of ethical ideology show different ethical attitudes, behaviors and judgments

in various contexts.

Figure 1 depicts our proposed model of observers' reactions to social-sexual behavior at work; its component parts and the hypotheses derived from it are discussed in the following sections.

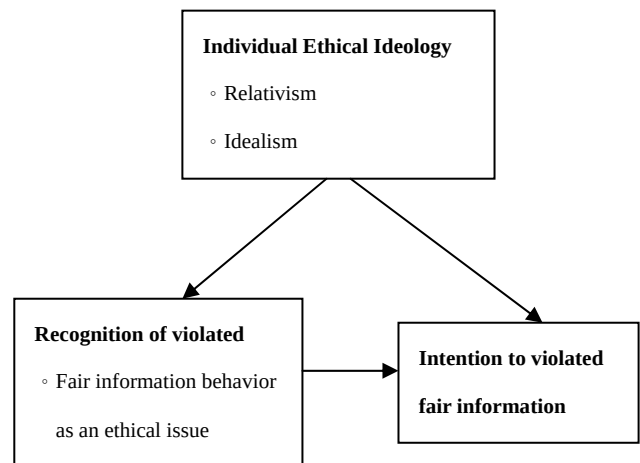


Figure 1: Research Framework

According to Schlenker and Forsyth (1977), individual differences in moral judgments can be described in terms of two ethical ideologies, relativism and idealism. Research indicates that individuals' ethical ideologies influence their opinions of contemporary moral issues, moral judgments of others, attributions of responsibility in response to wrongdoing, and reactions to their own moral failings (Forsyth, 1992). We believe that these factors are relevant to IS professionals' ethical decision making. Individuals who are highly relativistic do not believe in universal moral rules, whereas those who are less relativistic adhere to moral absolutes (Forsyth, 1980). More relativistic individuals may be less inclined to recognize violated fair information behavior as an ethical issue or to intervene in the behavior because they wish to know the complete context surrounding any such behavior. In contrast, less relativistic individuals may be more inclined to respond to violated fair information behavior because they have a set of predetermined rules that governs their responses to behavior that they deem inappropriate.

Proposition1: IS professionals' relativistic ethical orientations are negatively related to their (a) recognition of violated fair information behavior as an ethical issue, and (b) intentions to violated fair information.

Individuals who are highly idealistic believe that desirable outcomes can always be achieved, whereas individuals who are less idealistic believe that the "right" action often results in both positive and negative consequences (Forsyth, 1980). Trevino and Youngblood (1990) found that individuals' outcome expectancies influenced ethical behavior such that those who expected more positive outcomes were more likely to behave ethically. Thus, more idealistic individuals may be more likely to recognize social behavior as an ethical issue and to intervene in the behavior because they believe that their involvement will yield positive consequences. On the other hand, less idealistic individuals may be more likely to focus on potential negative outcomes of their involvement.

Proposition2: IS professionals' idealistic ethical orientations are positively related to their (a) recognition of violated fair information behavior as an ethical issue, and (b) intentions to violated fair information.

Ethical decision making models (e.g., Jones, 1991; Rest, 1986; Trevino, 1986) have proposed that cognitions regarding ethical issues are antecedents of intentions to act ethically and ultimately ethical behavior. In our model, the cognition of interest is the extent to which individuals perceive an incident of violated fair information behavior as an ethical issue and the intention of interest is the extent to which they intend to violated fair information the incident. Intentions may be defined as "a measure of the likelihood that a person will engage in a given behavior" (Ajzen & Fishbein, 1980: 42), or the self-perceived likelihood of taking an action. When forming intentions, individuals weigh the moral dimensions associated with a particular action or behavior against other decision dimensions such as economic,

social, and political (Rest, 1986). Therefore, rather than being solely idealistic, individuals also consider their own self-interest when establishing intentions. This notion is echoed in the social psychology literature. According to the theory of planned behavior (Ajzen, 1985), intentions are influenced by perceived behavioral control, which represents the perceived ease or difficulty of performing the behavior and reflects past experiences as well as anticipated obstacles (Beck & Ajzen, 1991:286). Further, support for the notion that framing an incident as an ethical issue is likely to lead to intentions to intervene in the incident is found in the literature on cognitive dissonance. The theory of cognitive dissonance (Festinger, 1957) states that individuals strive to maintain consistency between their various attitudes and their behavior. Individuals, who believe that an incident they witness is unethical but fail to establish intentions to do something about it, are likely to experience cognitive dissonance. Therefore, to minimize the stress and other negative feelings associated with cognitive dissonance, it is likely that individual who perceive an incident of violated fair information behavior as an ethical issue will feel compelled to do something about it. This argument is consistent with the finding that moral obligation is highly correlated with intentions in a variety of situations (Beck & Ajzen, 1991). For the reasons described above, it is expected that:

Proposition3: IS professionals' recognition of violated fair information behavior as an ethical issue is positively related to their intentions to violated fair information.

Conclusion

Confidentiality issues seem especially important in EMR because the moral behavior is essentially relation with fair information. The framework presented here considered the kind of individual characteristics that may be most relevant to the intention of violation behavior.

The personnel issues associated with ethical behavior will be helpful given the role of people in confidentiality management. Given the paucity of research on the topic, lessons may be drawn from related areas in management research. This paper focused on individual level factors to explain violated fair information behavior.

1. Implications for management

How do we link patient record, yet mitigate confidentiality concerns? How do we associate patient information accurately with the proper patient record, yet protect patient anonymity? How can we maximize the benefit of EMR and eliminate risks? Some of the alternatives to individual characteristics include the use of patient demographic information for indexing, searching and matching. This will subject the patient information to greater privacy risks. Some of those who are concerned with the confidentiality risks recommend these alternative methods to prevent unauthorized access. However, information technology (IT) is rapidly becoming so powerful and sophisticated that these methods will not be adequate as barriers to prevent unauthorized access. Provider organizations will find it difficult to monitor and exercise control. Therefore, developing security procedures and instilling responsibility among individuals required to overcome the confidentiality challenges.

We can also deduce some guidelines on confidentiality from the framework presented. For example, technical and industry knowledge can be acquired through formal training. A number of skills and competencies can be increased through training and development. Political, negotiating, and championing skills can be taught. Firms have two choices in addressing the need to have a pool of qualified individuals for the role.

One important moderating factor in selecting management potential is the learning ability of individuals. Prior research has documented that some

individuals may be better at learning from the experiences the organization offers them than others. McCall, 1994 found that an individual's ability to learn from experience is affected by such factors as curiosity; a sense of adventure; are not threatened by criticism and is open to feedback; accept responsibility for learning and change; and seeks and uses feedback. Individuals who rank high on ability to learn from experience will tend to benefit from the exposure designed to enable individuals acquire alliance management skills.

2. Implications for research

The discussion highlights several areas worthy of further study. The whole proposition generated here awaits empirical verification. This article looked at dispositional factors. The suggestion has been made elsewhere in the paper that dispositions may be a more important factor than situational factors in explaining behavior. At the same time, it will be instructive to look at the interaction of individual characteristics and parent firm cultures to see how they interact to affect violated fair information behavior. This research provides a preliminary list of personal characteristics hypothesized to be useful to confidentiality concern in EMR. Empirical testing of these and similar constructs would be useful.

Our knowledge of other important confidentiality issues on EMR may be rudimentary. For example, the present research omitted looking at the negative aspects of certain forms of disposition. Individuals with high initiative may push the relationship in ways unanticipated by violate fair information. In other words, such individuals are more likely to engage in "excesses." These and similar issues are worthy of our immediate research attention. Looking at those key individuals who play such a crucial role is one important place to focus. Such a focus should have important payoffs for our understanding of confidentiality on EMR.

Reference

Please contact with authors if readers are interesting to related references.