How do patients respond to violation of their information privacy?

Kuang-Ming Kuo, Chen-Chung Ma & Judith W. Alexander

Abstract

The introduction of electronic medical records (EMRs) can expose patients to the risk of infringement of their privacy. The purpose of this study was to explore the relationship between patients’ concerns about information privacy and their protective responses. A questionnaire survey conducted in a Taiwanese hospital revealed that, regarding information privacy, patients’ concerns about the collection of information about themselves, the secondary use of this information and the possibility of errors in the recorded information were associated with their information privacy-protective responses, while concern for unauthorised access to their information by other staff in the medical facility was not. Medical facilities should devote every effort to alleviate patients’ concerns about the invasion of their information privacy to avoid eroding the reputation of medical facilities and impeding the promotion of EMRs.

Key words (MeSH):

Electronic Medical Records; Privacy; Patient Data Privacy; Information Management; Computer Security

Introduction

Health information technology has become increasingly important to the healthcare industry because of its ability to lower costs, improve the efficiency of service delivery, enhance the quality of care and increase patient satisfaction (Rothstein 2007; Sykes, Venkatesh & Rai 2011). One example of these initiatives is the adoption of electronic medical records (EMRs) (Institute of Medicine 1997; Rothstein). EMR systems organise and store medical records electronically (Sykes, Venkatesh & Rai 2011) and function as the central information storage facility associated with patient care (Institute of Medicine 1997). By providing timely access to patient health information and decision support mechanisms, EMRs potentially reduce variability in the care of patients and are capable of enhancing the quality of decision making in clinical practice if properly implemented (Institute of Medicine 1997; Sykes, Venkatesh & Rai 2011; Zhou et al. 2009).

In spite of the potential benefits of EMRs it is inevitable that patients and others will raise ethical issues, including concerns about privacy, in this information age (Rothstein 2007). Privacy has been defined as ‘one’s ability to control information about oneself’ (Bélanger & Crossler 2011: 1018); it is violated when people cannot control their interactions with social and physical environments (Culnan 1993). In fact, privacy concern is not a new phenomenon; it often arises when the public perceives a threat from advances in information technology, which enable stronger capabilities for collecting, storing, and analysing personal information (Culnan 1993). Researchers have found increasing concerns about whether individuals are capable of protecting their personal private information (van Slyke et al. 2006), including personal health information (Institute of Medicine 1997; Rindfleisch 1997; Rothstein 2007).

In the context of health information, privacy refers to the ability of individuals to prevent the revelation of personal data to any other entity (Rothstein 2007). In general, medical data are considered to be more sensitive than other types of information (Malhotra, Kim & Agarwal 2004). Medical records contain a great deal of information about individuals, such as basic health information about height, blood pressure
readings, weight readings, and other vital signs (Rindfleisch 1997). They may also include
the most sensitive personal information, such as sexually transmitted diseases, Human
Immunodeficiency Virus (HIV) status, abortions, emotional problems, physical abuse,
and genetic predispositions to diseases (Rothstein 2007). If information such as this is
not well controlled and disclosed inappropriately, individuals may be exposed to serious
harm (Rindfleisch 1997). This situation may happen whether the medical records are
paper-based or computerised (Gostin et al. 1993). Moreover, the development of longitu-
dinal and extensive EMRs will greatly expand the scope and volume of health information
easily accessible in medical records (Rothstein 2007). Although EMRs can decrease
degmentation and inefficiency of paper-based medical records, they are potentially
vulnerable to misuse by both authorized and unauthorized users, resulting in a significant
increase in people's concerns about information privacy (Institute of Medicine 1997).
More importantly, little is known about the extent of privacy violations in medical facili-
ties (Institute of Medicine 1997). Thus, researchers and health information technology
professionals must carefully address individual concerns about information privacy in
respect to EMRs.

The aim of this study was to investigate the influence of patients' concerns about
information privacy on their protective responses, specifically in relation to EMRs.
The study is intended to assist governments, policy makers and medical facilities to
formulate improved strategies to protect patients' information privacy.

Conceptual framework and research hypotheses

We used a conceptual framework that contained the important factors influencing
patients' information privacy concerns. The theoretical framework was derived from
protection motivation theory (PMT) (Rogers 1975, 1983), and concern for information
privacy (CFIP) (Smith, Milberg & Burke 1996). We defined information privacy concern
as individuals' concern for information privacy regarding medical facilities' use and protec-
tion of their personal information. Information privacy-protective responses (IPPR) refer
to a set of behavioural responses of patients to their perception of information privacy
concerns resulting from information practices of medical facilities.

Protection motivation theory

Rogers (1975, 1983) introduced PMT to demonstrate how individuals alter their health
attitudes and behaviours in response to health-risk messages (Lee, Larose & Rifon 2008).
PMT suggests that cognitive appraisal of threats can arouse protection motivation,
which then focuses attention on understanding how individuals manage their percep-
tions of these threats and their mental coping mechanisms (Lee, Larose & Rifon 2008).
Specifically, when a message is perceived to be a serious threat, individuals understand
that threat as sufficiently terrifying to stimulate them to avert the threat (Youn 2009).
Previous researchers (Lee, Larose & Rifon 2008; Youn 2005, 2009) have used PMT to
explain risky behaviour and to generate effective messages to inhibit such behaviour. In a
similar manner, the present study adopted PMT to comprehend the propensity of patients
to use protection responses to avert privacy loss caused by the information handling
practices of medical facilities. To the best of our knowledge, few previous studies
have investigated the coping behaviours of patients when they are confronted with the
potential violation of their privacy through EMRs.

Threats to EMR privacy

In the EMR context, PMT suggests that the extent of patients' concerns about privacy
triggers the use of risk-diminishing behaviours. The higher the level of individual concern
about the privacy of information-handling practices in a medical facility, the more likely
it is that individuals will try to employ privacy-protective behaviours (Rogers 1975,
1983). Thus, the present study considered the extent of privacy concerns as protec-
tive motivation that stimulates subsequent behaviours to deal with information privacy
threats.
Concern for information privacy

Smith, Milberg and Burke (1996) proposed that an individual’s concern for information privacy (CFIP) is a general concern about how organisations use and protect personal information. CFIP suggests that people with substantial information privacy concerns perceive that: (a) more information about them is collected than is necessary; (b) personal information is used for undisclosed purposes; (c) personal information is not sufficiently protected from unauthorised access; and (d) the larger proportion of collected data are inaccurate (Smith, Milberg & Burke 1996; Stewart & Segars 2002). Specifically, CFIP is a multidimensional construct consisting of four dimensions: collection, secondary use, unauthorised access, and errors (Smith, Milberg & Burke 1996).

Protective responses to violation of information privacy

Individuals who have high levels of information privacy concerns tend to hold the view that organisational mishandling of their personal information can have substantial negative health outcomes (Dinev & Hart 2006; Smith, Milberg & Burke 1996; van Slyke et al. 2006). Applying the PMT to this proposition, individuals would take protective actions to minimise such information privacy risks. In other words, they are prone to engage in some types of information privacy-protective responses (IPPR) in response to the mishandling of their personal information by an organization (Son & Kim 2008). For example, these individuals are apt to ask organisations to eliminate their personal information from databases (Milne, Rohm & Bahl 2004), to share negative experiences with their relatives or close friends (Son & Kim 2008), or to speak against organisations that pose threats to their information privacy (Smith, Milberg & Burke 1996).

CFIP can be viewed as perceived threats to an individual’s information privacy regarding EMRs that also triggers the individual’s protective responses using PMT. Thus, the present study proposes the research framework outlined in Figure 1, which we used to formulate four hypotheses.

Concern for Information Privacy (CFIP)\(^a\) Protection Motivation Theory (PMT)\(^b\)

- Collection
- Unauthorised access
- Secondary use
- Errors
- Information Privacy-Protective Responses (IPPR)

\(H_1\)
\(H_2\)
\(H_3\)
\(H_4\)

Note. \(^a\)Smith, Milberg and Burke (1996); \(^b\)Rogers (1975, 1983).

Figure 1: Research framework

Research hypotheses

The effect of collection

Individuals are often aware that a great deal of information is collected about them (e.g. personal characteristics and background), which can be considered as a troubling
invasion of privacy and likely to arouse the concerns of most people (Milberg, Smith & Burke 2000; Sarathy & Robertson 2003; Smith, Milberg & Burke 1996). People are concerned about the extensive amount of personally identifiable data collected and stored in EMRs (Smith, Milberg & Burke 1996). Stone et al. (1983) included information collection as one component of information privacy. Smith, Milberg and Burke also proposed that information collection is one of the four dimensions of people’s concern for information privacy. Stewart and Segars (2002) argued that people’s privacy concerns might relate to specific information practices, including methods of collection. The ease of collection, storage, and transmission of data over electronic networks also creates significant risks to privacy (Gostin et al. 1993).

When applying PMT to the context of information privacy, it seems reasonable to expect that the collection of patients’ information by medical facilities will continue to be an important source of privacy concerns among patients (Malhotra, Kim & Agarwal 2004), which may lead to patients’ protective responses. Therefore, the first hypothesis postulates that:

\[ H_1: \text{There is a positive relationship between collection and patients' information privacy-protective responses} \]

The effect of unauthorised access

One goal of EMRs is to increase the accessibility and sharing of medical records among authorised individuals and medical facilities (Barrows & Clayton 1996). The integration of an individual’s information from various databases makes computerised health information increasingly valuable and thus requires perfect protection from unauthorised access (Institute of Medicine 1994). Unauthorised access refers to people’s concern that data about them are readily available to people not properly authorised to view or work with these data (Smith, Milberg & Burke 1996). In the healthcare context, one third of medical professionals have indicated that information is released to unauthorised people ‘somewhat often’ (Barrows & Clayton 1996). Although there is a general assumption that individuals should have a ‘need to know’ before they are permitted to access personal information (Milberg, Smith & Burke 2000; Smith, Milberg & Burke 1996), there is the possibility of threats to the privacy of information held in medical facilities from insiders who may gain unauthorised access to data via technical or other means (Institute of Medicine 1997). For example, the staff of information system departments may have access to other employees’ healthcare records where access is not properly controlled. The existence of information privacy rights means that someone has a duty either not to disclose information or to prevent unauthorised access to information by others (Institute of Medicine, 1994). Even lay people are concerned about unauthorised access to their personal information (Institute of Medicine 1994). Thus, it is critical to guarantee the availability of health data for authorised users and prevent leaking of information by unauthorised users (Barrows & Clayton 1996).

According to PMT (Rogers 1973, 1985; Son & Kim 2006), the greater the concern individuals have about their perceived information privacy, the more likely it is that they will take protective measures in response to that threat. Thus, the present study hypothesises the following:

\[ H_2: \text{There is a positive relationship between unauthorised access and patients' information privacy-protective responses} \]

The effect of secondary use

Occasionally, information about individuals is collected for one purpose but used for another, secondary purpose without permission from the individuals concerned (Milberg, Smith & Burke 2000), and concerns about privacy tend to be exacerbated when information is not restricted solely to the original purpose for which it was collected in the prime transaction (Sheehan & Hoy 2000). Therefore, if organisations process information beyond that required by the prime transaction, people’s concerns about privacy issues may increase (Nowak & Phelps 1995). Even if the information is controlled internally within the one organisation, the use of personal information without authorisation will often evoke a negative response (Milberg, Smith & Burke 2000). In the present study, secondary use refers to people’s concern that personal health information is collected
from the individual for one purpose but is used for another, secondary purpose without
the individual's authorisation (Smith, Milberg & Burke 1996).

In the context of health information, although medical records are designed to be
used within healthcare settings, health information may be legitimately acquired and
utilised by other organisations, since the value of such information is important and
increasingly used in decision-making (Rothstein 2007). Probable secondary users may
include insurers, pharmaceutical payers, employers, and other stakeholders in the
health information services industries (Rindfleisch 1997). In fact, few comprehensive
controls currently exist to ensure that an individual's health information is utilised only
for authorised purposes (Institute of Medicine 1997). Patients generally understand that,
with consent, information in their medical records will be shared widely within a hospital
and for insurance and reimbursement purposes. They also expect that data collected
about them will be used only for the purpose of the initial collection and that such data
will be shared with others only for that same purpose (Gostin et al. 1993; Institute of
Medicine, 1994). However, most people prefer to give permission prior to the use of their
health information for any purpose other than medical treatment (e.g. research) (King,
Brankovic & Gillard 2012). The use of personal information for other purposes without
authorisation will often arouse negative responses from individuals (Smith, Milberg &
Burke 1996).

Thus, according to PMT, the greater an individual's concerns about the secondary use
of their personal health information by medical facilities, the more likely it is that the
individual will try to respond with privacy protection behaviours (Rogers 1973, 1985; Son
& Kim 2008). Therefore, we propose the hypothesis:

\[ H_3: \text{There is a positive relationship between secondary use and patients'} \]
\[ \text{information privacy-protective responses.} \]

The effect of errors

Within the context of this study, error refers to intended and unintended errors in the
personal medical information collected about patients by medical facilities, and to
corns that individuals may have that protection against such errors occurring is insuf-
ficient (Smith, Milberg & Burke 1996). People may know that information about them is
being collected (Sheehan & Hoy 2000) but they may have concerns that the organisations
involved are not taking adequate steps to reduce problems that contribute to errors in
personal data (Milberg, Smith & Burke 2000; Smith, Milberg & Burke 1996). Although
some errors may be deliberate, most privacy-related concerns originate from accidental
errors in personal data (Milberg, Smith & Burke 2000; Smith, Milberg & Burke 1996).

Even in the healthcare industry, many medical records include errors and omissions
(Rothstein 2007). Errors in medicine are common and frequent, as they are in all areas in
life (Bates et al. 2001). Such errors occur regardless of whether personal health informa-
tion is paper-based or digitised. Theoretically, electronic patient data can be assumed
valid since medical information systems have undergone various quality-assurance proce-
dures such as software testing and verification (Barrows & Clayton 1996). Nevertheless,
errors in data integrity resulting from human error and/or malfunctions of healthcare
information systems will continue to occur (Barrows & Clayton 1996). While most errors
have little potential for harm, some do cause injury; thus the cumulative results of error
in healthcare may be enormous (Bates et al. 2001).

According to PMT, the greater the individuals’ concerns are about the potential errors
in EMRs, the more likely these individuals will try to utilise privacy protection behaviours
(Rogers 1973, 1985; Son & Kim 2008). Based on the discussions above, we hypothesise:

\[ H_4: \text{There is a positive relationship between errors and information privacy-}\]
\[ \text{protective responses.} \]
Method

Sample and data collection
To empirically validate the proposed hypotheses, patients over 18 years of age from a medical centre in southern Taiwan with a capacity of near 1,300 beds were selected. This medical centre was chosen for two main reasons: (a) the subject hospital provides nearly all necessary medical services, which attracts an average of nearly 5,000 outpatients each day; and (b) the subject hospital is equipped with a well-established EMR system that provides patients with high quality services. Prior to conducting the interviews and disseminating the questionnaires, the researchers received ethics approval from the Medical Records Department of the hospital. The Mall Intercept face-to-face interviewing method was adopted for data collection (Bush & Hair 1985). This methodology was used due to a lower refusal rate than has been found with other data collection methodologies (Bush & Hair 1985). Four trained interviewers recruited patients randomly at four main entrances to the medical centre from 1 January to 28 February 2012. Interviewers collected data via 5 to 10 minute face-to-face interviews with each respondent.

Measures
The questionnaire used in this study consisted of two parts. The first part collected the demographic data of respondents and the second part dealt with their perceptions about information privacy concerns and corresponding information privacy-protective responses. According to Churchill’s (1979) approach for generating questionnaires, the study combined scales from other relevant empirical studies to generate an initial pool of 21 items. Four of the items measured collection; four measured secondary use; three measured unauthorised access; four measured errors, and six were related to information privacy-protective responses. All 21 measures used a 5-point Likert-type scale (1 for strongly disagree and 5 for strongly agree) and were translated into Chinese for data collection. Ten volunteer patients pre-tested the questions to eliminate ambiguous words and phrases. Appendix I shows the final 21 items.

The CFIP scale for information privacy concern
CFIP, a multi-item scale first proposed by Smith, Milberg and Burke (2000) measures the concerns individuals have with the information privacy practices of organisations. CFIP is more widely used than other scales for assessing privacy (Bélanger & Crossler 2011). The scale has four dimensions, including collection of data, secondary use of data, unauthorised access to data, and errors in data. These four dimensions appear to provide a complete framework for information privacy concerns, and many researchers have cited their sound psychometric properties (Milburg, Smith & Burke 2000; Stewart & Segars; van Slyke et al. 2006). The CFIP was adapted to the context of EMRs by the authors according to suggestions from a panel of experts.

Information privacy-protective responses scale
Measures relating to patients’ information privacy-protective responses (IPPR) were adapted from the scale proposed by Son and Kim (2008). The IPPR determines a set of patients’ behavioural responses to their perception of information privacy threats that result from the information practices of medical facilities (Son & Kim 2008). IPPR has six dimensions, including: patients’ refusal to provide their personal information to medical facilities; fabrication of patients’ personal information to medical facilities; asking for the removal of patients’ personal information; negative word-of-mouth messages to their friends; complaints submitted directly to medical facilities; and complaints submitted indirectly to third-party organisations. Son and Kim (2008) empirically validated the IPPR, and reported that the scale had good reliability and validity (Son & Kim 2008).

Data analysis methodology
We used structural equation modeling (SEM) for hypothesis testing. SEM enables researchers to answer a set of interrelated research questions in a single, systematic, and comprehensive analysis by modeling the relationships among multiple independent and dependent constructs simultaneously (Baguszi & Yi 2012). The proposed model and hypotheses were empirically validated using partial least square (PLS), a component-based SEM (Chin 1998), supported by SmartPLS® 2M3 software (Ringle, Wende & Will
2005). PLS was selected because the collected data were non-normal while PLS makes no distributional assumptions (Chin 1998). Moreover, the global fit measure GoF was used to validate the PLS model globally and was computed as

$$\sqrt{AVE \times R^2}$$

(Wetzels, Odekerken-Schröder & van Oppen 2009).

Note: AVE = average variance extracted

Results

Descriptive statistics

A total of 300 patients were invited to participate in the study, 204 of whom agreed to participate (response rate = 68%). A majority of the respondents (54.9%) were 30-59 years old, with 50.5% being male and 49.5% female. With regard to educational background, 58.8% of the respondents had an undergraduate degree, 31.4% had a master’s degree, and 9.8% had completed high school. This sample was consistent with the general population for Taiwan for gender, but generally younger and better educated.

Analysis results

Previous studies suggest a two-stage process for assessing PLS model structure, including (a) the measurement model and (b) the structural model (Chin 2010; Henseler, Ringle & Sinkovics 2009). The measurement model articulates the relationships between the latent variables and the measured (observed) variables, whereas the structural model articulates the relationships between the exogenous and endogenous latent variables.

Measurement model

The measurement model was tested to ensure that the constructs possess sufficient reliability and validity. Reliability is usually evaluated via individual item reliability and construct reliability. Individual item reliability was assessed by means of confirmatory factor analysis (CFA) implemented by PLS (Gefen & Straub 2005). All constructs are modeled as first order and reflective, because their measurement items are manifestations of these constructs and because these items co-vary (Chin 1998). The decision to retain items was based on Henseler, Ringle and Sinkovics’s (2009) recommendations with regard to the absolute standard outer loadings (>0.7), which resulted in three items being dropped, including one item (UA2) in ‘Unauthorised Access’, and two items (IPPR1 and IPPR2) in ‘Information Privacy Protective Responses’. A second-run CFA was performed and the results indicated that all loadings were higher than 0.7. Construct reliability was tested by assessing Cronbach’s $\alpha$ and composite reliability (CR) (Henseler, Ringle and Sinkovics 2009). Cronbach’s $\alpha$ was higher than the suggested value of 0.7 for all variables tested (Henseler, Ringle & Sinkovics 2009), while the CR of all variables was greater than 0.8, which is higher than the suggested cut-off value of 0.6 (Henseler, Ringle & Sinkovics 2009), indicating sufficient reliability of the measurement (Table 1).

Table 1: Inter-construct correlations and reliability measures

<table>
<thead>
<tr>
<th></th>
<th>AVE</th>
<th>CA</th>
<th>CR</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection (A)</td>
<td>0.68</td>
<td>0.84</td>
<td>0.89</td>
<td>0.82</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised Access</td>
<td>0.69</td>
<td>0.85</td>
<td>0.90</td>
<td>0.27</td>
<td>0.83</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary Use (C)</td>
<td>0.79</td>
<td>0.74</td>
<td>0.88</td>
<td>0.37</td>
<td>0.72</td>
<td>0.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Errors (D)</td>
<td>0.71</td>
<td>0.86</td>
<td>0.91</td>
<td>0.17</td>
<td>0.61</td>
<td>0.55</td>
<td>0.84</td>
<td></td>
</tr>
<tr>
<td>Information Privacy-Protective Responses (E)</td>
<td>0.69</td>
<td>0.84</td>
<td>0.90</td>
<td>0.24</td>
<td>0.54</td>
<td>0.48</td>
<td>0.46</td>
<td>0.83</td>
</tr>
</tbody>
</table>

Note: AVE: Average Variance Extracted; CA: Cronbach’s Alpha; CR: Composite Reliability
Diagonal is the square root of AVE.
Criteria for assessing validity include convergent validity and discriminant validity (Henseler, Ringle & Sinkovics 2009). Fornell and Larcker (1981) recommend that convergent validity can be justified via the average variance extracted (AVE). Results revealed that AVE ranged between 0.68 and 0.79, exceeding the cut-off value 0.5 (Fornell & Larcker 1981), and suggesting good convergent validity (see Table 1). Moreover, discriminant validity can be assessed by comparing the square root of the AVE and the correlations of the construct with the other constructs in the model (Fornell & Larcker 1981). Results indicated that none of the inter correlations of the constructs employed in the study exceeded the square root of the AVE for the construct (see Table 1), indicating satisfactory discriminant validity.

Structural model
Since consensus does not exist about the sample size of bootstrapping (Andreev et al. 2009), bootstrapping with 1,000 re-samples (Chin 2010) was used to assess the path significance. Test results from structural equation modeling analyses of hypotheses are summarised in Table 2, where the standardised path coefficients and t-values are shown. The four hypothesised links were all supported, with the exception of Hypothesis 2 (unauthorised access → IPPR). Further, the four antecedents jointly explained about 33% of variance of IPPR.

Table 2: Model statistics

<table>
<thead>
<tr>
<th>HYPOTHESES</th>
<th>PATH</th>
<th>PATH COEFFICIENTS</th>
<th>t-VALUE</th>
<th>RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Collection → IPPR</td>
<td>0.077 *</td>
<td>2.066</td>
<td>Supported</td>
</tr>
<tr>
<td>H2</td>
<td>Unauthorised access → IPPR</td>
<td>0.113</td>
<td>1.696</td>
<td>Failed to support</td>
</tr>
<tr>
<td>H3</td>
<td>Secondary use → IPPR</td>
<td>0.332 ***</td>
<td>4.267</td>
<td>Supported</td>
</tr>
<tr>
<td>H4</td>
<td>Errors → IPPR</td>
<td>0.177 **</td>
<td>2.821</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Note: * p < .05, ** p < .01, *** p < .001

As for the GOF, the geometric mean of AVE is 0.711 and $R^2$ is 0.334 in this study. Thus, the GOF for this study is 0.487, exceeding the cut-off value 0.36 for large effect sizes, indicating the model performs well (Wetzels et al. 2009).

Discussion

The effect of collection
Results for Hypothesis 1 support the proposition that a positive relationship exists between data collection and patients’ information privacy protection responses; that is, patients are concerned that too much of their personally identifiable information was collected by medical facilities. Also, the collection of their personal private information may cause patients to feel uncomfortable or embarrassed. These results are consistent with conclusions reached by previous studies (Malhotra, Kim & Agarwal 2004; Smith, Milberg & Burke 1996; Stewart & Segars 2002). To cope with this problem, Smith, Milberg and Burke (1996) further suggested that the database design for storing personal information should be parsimonious, collecting only required data. This suggests that EMRs in the hospital should collect only the minimal levels of data sufficient for treatment. However, the individual health conditions of patients should determine the amount and type of data to be collected including data on social support, living conditions, and previous diagnoses.

The effect of unauthorised access
In testing Hypothesis 2, the results failed to support the proposition. Patients in this study had little concern about unauthorised people within the hospital setting accessing their EMRs. These results are counter-intuitive. In fact, medical personnel have been found to often abuse their record access privileges out of curiosity or for their own purposes (Rindfleisch 1997). However, patients who attend medical facilities may have a high degree of trust in their physicians and in the interests of receiving adequate
treatment they may not be overly concerned about unauthorised access to their EMRs within these medical facilities. Moreover, many individuals may not understand how authorised or unauthorised users of medical facilities access their EMRs if medical facilities do not disclose the process of access to information. Finally, since most respondents were educated, they may have had a greater level of trust in their peers and therefore less concerned about unauthorised access by hospital staff. Thus, although the results of this study failed to confirm the relationship between unauthorised access and IPPR, medical facilities should nonetheless keep track of the activities of EMR usage by authorised and unauthorised employees.

The effect of secondary use

With regard to Hypothesis 3, results revealed a positive relationship between secondary use and patients’ information privacy protective behaviours; that is, patients in this study did care about the use of the information in their EMRs when this secondary use was different from the original purpose. This result is consistent with conclusions reached by previous studies (King, Brankovic & Gillard 2012; Smith, Milberg & Burke 1996). These researchers suggested that medical facilities should refuse to release personal data to outside entities without prior approval and consent; that is, healthcare institutions should never deliver personal health information to other individuals or organisations without the individual’s consent and acknowledgement of hospital management. Currently, many potential secondary users of health information (e.g. insurers, pharmaceutical payers) exist. These users have a justified need to access personal health information; however, few procedures are in place to ensure that the information is used solely for intended purposes (Rindfleisch 1997). Medical facilities should address this situation with care when implementing EMRs.

The effect of errors

Results of Hypothesis 4 support the proposition that a positive relationship exists between errors in EMRs and patients’ information privacy protective behaviours. In other words, patients care about the accuracy of information in their EMRs because they want their physicians to make medical decisions based on reliable and confident data (Institute of Medicine 1994). In the era of EMRs, patient information can easily be sent to other medical facilities. If the information is somewhat fallacious and not corrected in a timely manner, the impact on the patient safety may be great. This finding is consistent with conclusions confirmed by Smith, Milberg and Burke (1996). Moreover, one of the goals of information privacy is to ensure the integrity of healthcare data (Barrows & Clayton 1996). Patients cannot possibly review and correct data about themselves (Gostin et al. 1993); thus, the subject hospital should protect EMRs from intended or unintended alterations to maintain data accuracy, completeness, and integrity (Barrows & Clayton 1996; Gostin et al. 1993; Institute of Medicine 1994).

Implications and limitations

Practical implications

First, the present study, which identified the central dimensions of patients’ information privacy concerns about EMRs (i.e. collection, secondary use, and errors), can serve as the first step on a path of proactive management towards this issue (Smith, Milberg & Burke 1996). Moreover, the present study also found that patients took protective responses towards EMRs when their information privacy concerns were invaded. The lack of attention to these relationships in the healthcare context is problematic because of the influence of these relationships on the promotion of EMRs in the future. Thus, these findings may assist the development of EMRs by those responsible for formulating and implementing information-privacy protection procedures in organisational and societal contexts. Additionally, legislators could use these results to guide the formulation of information-privacy protection-oriented legislation (Stone et al. 1983).

Theoretical implications

Previous studies have emphasised the relationship between people’s information privacy concerns and information privacy protective behaviours (Lee, Larose & Rifon 2008; Youn 2005, 2009). However, researchers have conducted minimal research in the health-
care context regarding people’s information privacy concerns about EMRs. Thus, more privacy studies using a conceptual framework similar to the one used in this study should examine the crucial role that information privacy concerns have in shaping people’s attitudes toward EMRs.

Limitations of the study
This study only looked at people who access EMRs without authorisation as staff at the medical facility, which might ignore other unauthorised access by individuals not associated with the medical facility. Further, the external validity of the findings may be limited as the sample was collected from one hospital in Taiwan only. Consequently, inferences to other populations cannot be made safely. However, the collected sample possessed certain demographic characteristic (e.g. gender) in the same proportion as the Taiwanese population, although there were some differences in age and education, meaning that these results may be generalisable to other Taiwanese hospitals. Future research could expand on the present study’s findings by using a more representative sample in other geographical settings.

Conclusion
This study investigated relationships between patients’ information privacy concerns and their information privacy protection responses towards EMRs, based on protective motivation theory. Results indicated that collection of information, secondary use of information and errors in data collection were primary factors in arousing patients’ information privacy protective responses toward EMRs.

Governments and medical facilities should focus on these findings and develop EMR privacy protection policies to reduce people’s information privacy concerns. From a theoretical perspective, this study contributes to CFIP literature by further exploring the relationship between patients’ information privacy concerns and their information privacy protective responses. Furthermore, this study has empirically validated the appropriateness of employing the CFIP instrument in a health care context. Additionally, because the number of medical facilities adopting EMRs has risen, studies on patients’ views about information privacy have become increasingly important. This study makes a contribution to filling this research gap.

References


Kuang-Ming Kuo Ph.D.
Assistant Professor, Department of Healthcare Administration
I-Shou University, Kaohsiung City
Taiwan, Republic of China
email: kmkuo@isu.edu.tw

Corresponding author
Chen-Chung Ma Ph.D.
Assistant Professor, Department of Healthcare Administration
I-Shou University, No.8, Yida Rd., Yanchao District
Kaohsiung City 82445
Taiwan, Republic of China
Tel: +886-7-6151100 ext. 7614
Fax: +886-7-6155150
email: up000238@isu.edu.tw

Judith W. Alexander Ph.D.
Emerita Professor of Nursing
University of South Carolina, Columbia
United States of America
email: jwalexan@mailbox.sc.edu
### Appendix I. Questionnaire items

<table>
<thead>
<tr>
<th>DIMENSIONS</th>
<th>ITEM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection (CO)</strong>&lt;br&gt;(Smith, Milberg &amp; Burke 1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It bothers me when medical facilities ask me for personal information.</td>
</tr>
<tr>
<td></td>
<td>I sometimes think for a while when medical facilities ask me to provide personal information.</td>
</tr>
<tr>
<td></td>
<td>It bothers me to give personal information to so many medical facilities.</td>
</tr>
<tr>
<td></td>
<td>It bothers me that medical facilities collect too much personal information.</td>
</tr>
<tr>
<td><strong>Unauthorised Access (UA)</strong>&lt;br&gt;(Smith, Milberg &amp; Burke 1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical facilities should devote more time and efforts to preventing the unauthorised access of patients’ personal information.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should prevent unauthorised people from accessing patients’ personal information without considering the cost.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should take more measures to ensure that unauthorised people cannot use their computer to access patients’ personal information.</td>
</tr>
<tr>
<td><strong>Secondary Use (SU)</strong>&lt;br&gt;(Smith, Milberg &amp; Burke 1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical facilities should never use patients’ personal information for purposes other than medical care, unless it has been authorised by the patient.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should not use the personal information provided by patients for any purpose other than those required for medical care.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should never sell patients’ personal information to other institutions.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should not share patients’ personal information with other institutions unless it has been authorised by the patient.</td>
</tr>
<tr>
<td><strong>Errors (ER)</strong>&lt;br&gt;(Smith, Milberg &amp; Burke 1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical facilities should repeatedly check the accuracy of patients’ personal information without considering cost.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should use more procedures to ensure the accuracy of patients’ personal information.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should have a more comprehensive procedure to correct for errors in patients’ personal information.</td>
</tr>
<tr>
<td></td>
<td>Medical facilities should devote more time and manpower to verify the accuracy of patients’ personal information.</td>
</tr>
<tr>
<td><strong>Information Privacy-Protective Responses (IPPR)</strong>&lt;br&gt;(Son &amp; Kim 2008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I would refuse to provide information to medical facilities because I think it is too private within the next three years.</td>
</tr>
<tr>
<td></td>
<td>I would misrepresent some of my personal information if it is requested by medical facilities within the next three years.</td>
</tr>
<tr>
<td></td>
<td>I would take some actions to have my private information removed from medical facilities’ EMR database when it was not properly manipulated.</td>
</tr>
<tr>
<td></td>
<td>I would speak to my acquaintances about my poor experience with medical facilities’ mishandling of my personal information.</td>
</tr>
<tr>
<td></td>
<td>I would contact medical facilities to complain about the way they mishandle my personal information.</td>
</tr>
<tr>
<td></td>
<td>I would contact an elected official or consumer protection organisations to complain about the mishandling of my personal information by medical facilities.</td>
</tr>
</tbody>
</table>