Electronic Privacy: Patient Concerns

Anza A. Akram
University of California Riverside

Follow this and additional works at: https://scholarworks.lib.csusb.edu/ciima

Part of the Management Information Systems Commons

Electronic Privacy: Patient Concerns

Anza A. Akram
Lecturer, Anderson School of Management,
University of California Riverside, Riverside, CA 92521-0123
909 641-6564;
anza@sbcglobal.net

ABSTRACT

This study postulates issues related to electronic privacy and addresses the factors that directly effect personal electronic information. There is no positivist study done to measure patient privacy concerns using Smith et a l(1996) privacy model and the effect of previous experience and media on these concerns. This study measures the four dimensions of patient concerns against the electronic privacy, defines as the automation of patient records, meaning that computerized patient records will be signed, modified, authenticated, stored, and retrieved via computer. The defined model uses multiple constructs with multiple indicators and thus, Partial Least Square (PLS) is applied to study the relationships between the model variables. The electronic privacy resides inside the databases is secured by using various electronic security systems that are implemented and maintained by the organizations. The merging, acquisitions and strategic alliances to gain a competitive edge in the market raise a fear of data ownership and its distribution for unauthorized purposes. If not properly defined to the organizations, the electronic privacy can not be protected even in the presence of highly sophisticated hardware and software technologies.

Keywords: Electronic records, privacy, Collection, Error, Media

INTRODUCTION

Privacy, confidentiality, and security in an age of automation is an increasing concern to the American public and to congressional leaders (Simpson 1994). The Harris-Equifax Health Information Privacy Survey of 1993 showed that more than 80 percent of American public have high levels of concern about personal privacy and 60percent have concern about the usage of their medical records for any other reason (Simpson 1994). Critics are concerned about the delay in call for the reforms of privacy legislation and suggest an immediate action. "Making privacy seem like an afterthought will breed public distrust at a time when the public already is skeptical about the ability of government and business to keep sensitive data confidential, according to interest groups ranging from hospital administrators to the American Civil Liberties Union" (Betts, 1993).

Recently, to have a better grasp of privacy issues Healthcare organizations have created a new Executive positions, Chief Privacy Office (CFO), to report directly to Chief Executive Officer, to address the issues faced by setting sound policies and introducing better practices to provide the best possible services to their customers. The recently described position and absence of hard facts regarding the position to predict the importance of role and effectiveness is questionable. In spite of the concerns the recognition of the problem by the organizations is encouraging and contributes towards the efforts that have been made to regulate the privacy issues.

Dissipation of information using different channels always makes the issue more visible and understandable to the general public. Previous research shows that media plays a major role in effecting the opinion of the public. A compatible platform, Television and other electronic media are pushing a massive quantity of information and misinformation quicker than ever at the public (Hoke, 1998). The critical nature of the issue has challenged the ability of media to influence the opinion of the public and identify the importance of viewpoint of the health care revolution (Ignagni, 1998).Although the intention of the media is to dissipate the news and not to influence the opinion but the combination of avoiding a responsibility and using their own resources to establish a better understanding, public in most of the cases believe what they are told and thus, make the role of media more critical and sensitive. Health care industries recognize the powerful role of the media and try to better communicate with

media. Patients receive most of the information about healthcare and policy makers through media (Ignagni, 1998). It is thus, not improper to say that media coverage regarding privacy practices of medical information can effect patient concerns both negatively or positively and makes it an interesting and valuable variable to study.

A new survey of 260 hospital by the Chicago computer law firm Gordon & Gordon suggests that some hospitals would need to beef up their security policies with the Condit bill as 28% do not have a written policy on patient information, and only 43% have audit trails to track access to sensitive information (Betts, 1994). The advances in the technology has brought noticeable change in the healthcare industry on how they handle the medical practices and the dependency on the technology. The information downloaded from the website of Health Tech (2004) and other literature in the field have discussed eye opening advances in the medical areas which definitely are impressive and progressive but raise various issues of concern when so many different platform are integrated together to make technology feasible and demanding. The response time is decreased and to address the issue is more interactive and responsive. The healthcare organizations have clinical engineers to work along with the team of physicians, nurses, technologists and other hospital staff (Grimes 2004). Grimes (2004) mentioned that complexity and sophistication of technology leads to significant number of medical errors and if cautious measures are taken to implement, is a productive partner to the medical team. Following are the details of the facts and various technologies used by the healthcare organization (HealthTech 2004, Grimes 2004):

Technologies	Description of Services
1. Point of Care Mobile Computing	Device to get clinical information instantly.
2. Point of Care	Remote Patient Management
3. Point of Care Testing	Remote Patient Management
4. Wireless[1] bar-code scanners.	
5. PDA	For medicines and other medical- care
6. Interactive Videoconferencing	
7. Forward Messaging	Store & real time dialogue sharing audio/ video conferencing equipment
8. Website Interaction	Asynchronous correspondence between individuals Asynchronous or real-time message correspondence between an individual and Web Site.
9. Delivery Robots carry cart (Advanced Technology Institute)	Delivery purposes
10. Clinical Data Entry	
11. Networking	
12. PACS	
13. Surgical Robotics	To assist in surgeries
14. Diagnostic Systems (Grimes 2004)	Imaging systems, Clinical labs, Physiologic monitoring systems
15. Therapeutic/ Treatment Systems (Grimes 2004)	Respiratory therapy, pacemakers, defibrillators, radiation therapy, infusion therapy.
16. Information Processing Systems (Grimes 2004)	DSS and AI systems to integrate clinical information with patient information to make decisions.

Table 1: Healthcare Technologies

---

[1] According to white paper of HealthTech (2004) the healthcare wireless market in 2003 was around $330 million and is predicted to go up to 637 million in 2007.

RAMIFICATION

The sophistication and integrations of healthcare technologies invite challenges and are sensitive to the threats that can jeoperdise the integrity of the healthcare databases. The ramifications to the data are discussed in Table 2:

Hacking	Due to the nature of information, security is major problem in the databases and other electronic devices.
Magnetic interferences	The noise in the system is serious issue when most of the communication is done through mobile systems and can provide incorrect and error while transferring from one node to another.
Lost of communication	Communication interruption can disrupt the process of medical care and can be devastating and establishing connection can be time consuming.
Distribution reliability.	Usage of distributed systems like mobile systems, connected databases, centralized and decentralized systems needs additional data scrubbing to ensure the data accuracy (Pearson 2002).
User Interfaces Usability	Design or Method issue (Orring and Vainio 1990)

Table 2: Ramifications

CONCEPTUAL MODEL

Laufer et al (1977) described privacy as a "Situation affecting an individual's perception and experience of privacy and invasions of privacy are described in terms of 3 dimensions: self-ego, environmental, and interpersonal". Warren et al (1977) suggested that privacy and secrecy both involve boundaries and denial of access to others. The ability to easily collect and correlate many diverse pieces of information from a variety of sources makes the revelation of any information the basis for a possible invasion of privacy (Warwick, 1997). Privacy is viewed, as a regulatory process that serves to selectively control access of external stimulation to one's self or the flow of information to others (Klopfer and Rubenstein 1977). Thus, privacy and secrecy both defines the richness of intensity a person encounters when the boundaries he or she defines are intentionally crossed and uninvited scrutiny threatens the safety[2].

Information privacy is commonly considered as a single-dimensional construct even if various studies have approached it multi-dimensional; however the specific dimensions differ from study to study (Smith et al, 1996) and are dependent upon the research questions and motive. Smith et al (1996) developed and validated an instrument to measure individuals' concerns about organizational information privacy practices. The development process included examinations of privacy literature and US laws; experience surveys and focus groups; and the use of expert judges. The researchers expected that this instrument would be used primarily in positivist studies. The process of instrument development and validation used in this study included steps that addressed not only a researcher's positivist understanding (e.g., a theory taking the form of independent and dependent variables or measurable objectivity) (Solem 2003), but also the subjective understanding (i.e., what the research subjects themselves understand their situation to be) as well as what researcher observes and interprets to be subjective understanding (Smith et al 1996).

This study measures the four dimensions of patient concerns against the privacy instrument developed by Smith et al (1996). Thus, the focus of the study is: (1) to validate the instrument developed by the Smith et al by identifying patient concerns regarding personal medical records electronic privacy; (2) to investigate the effects of previous experience and media, the independent variables, on privacy, the dependent variable.

Privacy Concern

---

[2] According to the Chamber's dictionary safety is" a state or fact of being safe". Data represent the physical coding (facts) of the patient and is major predictor of future treatment to be received in case of emergencies and other health related situations.

The four main dimensions of individuals' concerns about organizational information privacy practices identified by Smith et al (1996) are collection, unauthorized secondary use, improper access, and errors. While discussing the first dimension, collection, Smith mentioned in their study that the Association for Computing Machinery (ACM), a major association of information professionals, has a phase in its Code of Professional Conduct that dictates members shall "always consider the principle of the individual's privacy and seek ... to minimize the data collected...' There's too much damn data collection going on in this society (Smith et al 1996). The usage of integrated systems make the collection of data from different systems and sources readily available and less time consuming but on the other hand, due to insignificant connected sources the validity of collecting data is legally questionable (Pearson 2002).

Error is the second important dimension of privacy concern. In this case is described as an untrained employee who enters and distribute wrong information or creates two different records for the same patient with incorrect data. For example, "a clerk may not register a patient in the same way twice. Patient information then gets spread out over two records, so when clinicians go to treat the patient, they have an incomplete medical picture" (Simpson 1994). Technology complexity also makes the process of user interface hard to use and data error occurs due to untrained employee.

Unauthorized secondary use, third dimension of concerns, is sometimes raised with respect to combined databases that pull personal data from numerous other source, creating what has been termed a "mosaic effect" (Smith et al 1996).The different sources of data are linked together and belong to centralized and decentralized systems, though an intelligent ways of connecting databases, can be intrusive, ill-advised and incomplete if the concerned party is uninformed about the usage and the sources of the data. The linked data generates reports that provide a third type of data to physicians, retailers, health plans and employers and the method creates predictive models and decisions are made to project across larger population (Benzing 1994, Grimes 2004). Huff (1979) argues that strategic intelligence systems and its usage in complex environment challenge the regulations that needed to be shaped where privacy can easily be ignored and compensated for convenience and capacity in which organization can collect and generate interpretation. If not implemented precisely and tactfully, it can produce devastating result for the patient population. Telemedicine is a barrier to privacy, confidentiality and data security and raise various legal issues regarding computer-based medical records and documentation that has to comply with state laws regarding principles of documentation and under what conditions patient records may be stored in databases or as electronic records (Tyler 2001).

Improper access is a fourth dimension of privacy concern. Who within an organization is allowed to access personal information in the files? This is a question not only of technological constraints (e.g., access control software) but also of organizational policy. It is often held that individuals should have a "need to know" before access to personal information is granted (Smith et al 1996). Previous literature identified that privacy concerns like collection, errors, unauthorized use, and improper accesses are directly related to media (Hoke 1998, Smiley and Andsager 1998).

Based on the above information, the following hypotheses are proposed:

H1a: Media has a direct effect on concern about collection of medical data.
H1b: Media has a direct effect on concern about error in medical data.
H1c: Media has a direct effect on concern about unauthorized use of medical data.
H1d: Media has a direct effect on concern about improper access of medical data.

Previous Personal Experiences

It is believed that previous personal experiences may impact patient concern's about information privacy. Smith et al defined this variable as an antecedent variable. Individuals who had been exposed to or been victim of, personal information misuses should have stronger concern regarding information privacy (Smith et al 1996). Therefore, the proposed hypotheses are as follows:

H2a: Previous personal experiences have a direct effect on concern about collection of medical data
H2b: Previous personal experiences have a direct effect on concern about errors in medical data.
H2c: Previous personal experiences have a direct effect on concern about unauthorized use of medical data
H2d: Previous personal experiences have a direct effect on concern about improper access of medical data.

Media

Media coverage may increase the level of concern (awareness) about information privacy (Westin 1990) which was ignored in the past due to lack of data or information related to the experience. "The media, in its many cacophonous forms, is delivering the news, and it is not all good- or bad. The message is mixed, a confusing picture served up regularly on the nightly news. Journalists have an obligation to inform their readers, not just provoke them, to reach beyond the individual anecdote to report the entire story of managed care" (Iglehart, 1998). Thus, the following hypothesis is proposed:

H3: Media has a direct effect on previous personal experiences.

RESEARCH METHODOLOGY

Sample

The probability random sampling is used in this study. 300 surveys[3] were distributed randomly. The questionnaire survey (Appendix I) were collected through personal contacts and through mail. This provides a sufficient sample for the study. The contacted persons were the managers, decision makers and professionals. The intent of the study, in case of, personal contact was explained verbally, where the responses were collected through mail, a letter explaining the objective of the study and self-addressed return envelop were attached with the survey. The respondents was provided with a return envelope, with a return address and return postage. Putting stamps on the return envelopes seems to produce a small increase in return rates (Bickman and Rog 1998).

The personal channels were found more effective and the response rate was 80 percent. The survey that are collected through mail, the response rate was 2.5 percent. Overall 110 responses are received and were evaluated and there findings are discussed later.

Measures for Constructs Used in the Research Model

The measures for constructs are taken from Smith et al (1996). Some appropriate modification is done to make it specifically relevant to patient data. Each indicator is followed by a seven-point Likert scale ranging from "Strongly disagree" (1) to "Strongly agree" (7). Refer to the Appendix for a detail description of the study questionnaire.

Collection: This construct is defined as "concern that extensive amounts of personally identifiable medical data are being collected and stored in databases" (Smith et al 1996). Four items (Appendix I) comprise the subscale for this construct. The participants is asked to agree or disagree by selecting a point from a seven-point Likert scale anchored by Strongly disagree (1) and Strongly agree (7).

Errors: It is described as "concern that protections against deliberate and accidental errors in medical data are inadequate" (Smith et al 1996). Four items (Appendix I) comprise the Error subscale (Smith et al). Participants is asked to agree or disagree by selecting a point from a seven-point Likert scale anchored by Strongly disagree (1) and Strongly agree (7).

.

Unauthorized Secondary Use: Smith et al described it as "concern that medical information is collected from individuals for one purpose but is used for another, secondary purpose without authorization from the individuals." Four items (Appendix I) comprise its subscale. . The participants were asked to agree or disagree by selecting a point from a seven-point Likert scale anchored by Strongly disagree (1) and Strongly agree (7).

Improper Access: This measure is defined as "concern that medical data about individuals are readily available to people not properly authorized to view or work with this data" (Smith et al 1996). Three items (Appendix I)

---

[3] Educators from California State University San Bernardino (response rate 2.5%) and University of California Riverside (response rate zero).
Manufacturing Organization in Riverside (response rate 70%)
Members of Loma Linda Loopers (Running club; response rate 80%)
Group of Lawyers from Riverside (response rate 100%)

comprise the improper access subscale. Respondents were asked to agree or disagree by selecting a point from a seven-point Likert scale anchored by Strongly disagree (1) and Strongly agree (7).

Previous personal experience: This construct is defined as "previous personal bad or good experiences increase or decrease a level of concern regarding their information privacy. There is one indicator proposed by Smith et al (1996) to measure this construct. The following question will be asked: "How often have you personally been the victim of what you felt was an improper invasion of privacy?" The respondent is asked to answer the question by selecting one of the choice provided to them on a seven-point likert scale ranging from "never" (1) to "very great extent" (7).

Media: This construct is defined as "media coverage may increase the level of concern about information privacy (Smith et al 1996). There is one indicator suggested by Smith et al (1996) to measure this construct. The following question is asked: "How much have you heard or read during the last year about the use and potential misuse of computerized information about patient?" The respondent will be given a seven-point Likert scale ranging from "never (1) to "very great extent" (7).

DATA ANALYSIS

The statistical technique used to analysis data is a replication of statistical technique used by Igbaria et al (1997) except in this case SPSS software is used. Partial Least Squares (PLS) is used to study the model described in Appendix III, figure 1. It is a powerful approach to studying structural models involving multiple constructs with multiple indicators. PLS is a second-generation multivariate technique that facilitates testing of the psychometric properties of the scales used to measure a variable, as well as estimation of the parameters of a structural model, i.e. the strength positive or negative) and direction (direct or indirect) of the relationships among the model variables. It embodies two sets of equations representing the paths among the constructs/measures. The first set is measurement equations represent the relationships between the indicators/items and the second set is the relationship of variables that they measure (Igbaria et al 1997).

PLS allows the researcher to test the relationships within the measures (the measurement model) (Appendix III Fig I) and the hypothesized relationships between the measures (the structural model) (Appendix III Fig 2) simultaneously (Igbaria et al 1997, Igbaria and Greenhaus 1992). The test of the measurement model includes estimation of the reliability coefficients (composite reliability) of the measures, as well as, an examination of the convergent and discriminant validity of the research instruments (Igbaria et al 1997).

Discriminant validity assessment of the measures, i.e., the degree to which measurements differentiate among measures or measure distinct concepts, observation of the correlations between the measures of potentially overlapping measures is conducted (Igbaria et al 1997). If the items associated with a measure correlate more highly with each other than with items associated with other measures in the model, the measure is determined to have adequate discriminant validity (Igbaria et al, 1997).

The path coefficient of an exogenous variable represents the direct effect of that variable on the endogenous variable. An indirect effect represents the effect of a particular variable on the second variable through its effects on a third mediating variable. It is the product of the coefficients along an indirect route from cause to effect via tracing arrows I the headed direction only. When more than one indirect path exists, the total indirect effect is the sum. The sum of the direct and indirect effect reflects the total effect of the variable on the endogenous variable (Igbaria et al, 1997).

The measurement of privacy has high reliability and validity and found to be highly relevant measures for the privacy issues. H1 through H3 are rejected by the findings and no direct effect has been found. The findings sample is small and cannot be generalized and there is a need of larger sample size to study the effects and generalization. This study validates the instruments developed by smith et al and that privacy is multidimensional and the developed instrument are accurate and can be implemented in any industry and can help in developing policies around privacy and healthcare technologies if studied in depth.

STUDY RESULTS

The reliability analysis test in SPSS was selected to study the properties of measurement scales and the items. It calculates a measures of scale reliability (Appendix II table1) and the relationship between the items and relates to the consistency of the measures. The reliability exceeds the standards define by (Nunnallly 1978) and ranges from .907 to .941 and shows strong internal consistency reliability of the variables. The average variance matrix (Appendix II table 1) shows the covariate analysis to remove extraneous variation in the dependent variable due to one or more uncontrollable independent variables (Hair et al 1998). The Cronbach's Alpha based on the average inter-item correlation is .909 and indicates high reliability. The Values in table 2 depicts discriminant validity of the measures and the relationship of measures is strong with their associated items than the correlation between the other items.

The intercorrelation between the items (Appendix II, table 3) is high and positive and shows high predictivity of relevance between the measurements and the item being measured, privacy. The values range from .74 to .89. Whereas, the intracorrelation between the items (Appendix II, table 2) shows that the measures are less relevant and are not good predictor to measure the variables, previous experience and media. The reliability and validity of the privacy is strong as compare to other variables, personal experience and media. There is no significance relationship found between the hypotheses. Hypotheisis H1a through H3, range from -.05 to .47, are found not true. The previous experience and media has no direct effect on the privacy concerns. The media effect on the previous experiences though not significant still shows some direct effect.

LIMITATIONS OF THE STUDY

Previous experience and media needs to be defined more in depth conceptually and operationally. The item may be defined as multi-dimensional. The indicators to measure these two variables need to be reviewed again by researchers, professionals, academia and practitioners.

Implications for Researchers and Practitioners

This study provides information about patient concerns regarding their electronic data from a different prospective. Future research in the health care industry can benefit by focusing their research on the privacy model presented by this study and by including the patients' personality factors and future behavioral variables and study their relationships and effects on privacy model. They can also build on my model and use it in conducting interpretive studies. Moreover, other important relationship which is not studied in detail but needs technical and strategical attention are human-computer interaction wile collecting data (Orring and Larsson 1990) and the electronic agents search effects on privacy issue of an individual.

This study will bring the patient and health care closer by providing an awareness regarding patient privacy issues and will help policy makers to build their policies around the major concerns identified by the patients about their electronic data. This study will also provide a beginning point in looking at the factors like the effect of virtual societies on patient privacy and the policies and practices of health care industry to protect the confidentiality of the patient in electronically challenged environment.

CONCLUSION

Privacy issues are great concerns of the patient and the healthcare organization are taking measures to prevent any future consequences. The sophistication of technology and the ease of transfer of information and its usage will bring new challenges for the legislatures and the healthcare organizations. This study helps in determining the factors that increase the liabilities issues of the healthcare organizations and does provide an individual insight to evaluate these factors if needs arise and provide a different prospect to the patient and other decision makers to select better ways to address the issues, if any, occurs in the future.

REFERENCES

Advance Technology Institute. October 2002. "Protecting Privacy when using Telehealth Technology in Healthcare", http://tdrt.aticorp.org/privacydoc_vol1.html

Benzing, Lynn, MacKelvie, F. Charles. Nov 1994. "Coping with patient privacy", *Pharmaceutical Executive*, 14(11), pp. 63-74.

Betts, Mitch. Apr 11, 1994. "Health reform raises privacy issues", *Computerworld*, 28(15), pp. 55.

Betts, Mitch. Nov 22, 1993. "Privacy key to public trust in health care reform", *Computerworld*, 63, pp. 63.

Bickman, Leonard, Rog, J. Debra. *Handbook of Applied Social Research Methods,* Sage Publications, Inc. Thousands Oaks, Ca, 1998.

Connolly, Jim. July 6, 1998. "Health privacy model advances at NAIC", *National underwriter (Life/Health/Financial Services)*, 102(27), pp. 54-55.

Hoke, Henry Reed. Feb. 1998. "Privacy takes another hit", *Direct Marketing*, 60(10), pp. 4.

Huff AS. December 1979. "The future of organizational privacy". Information Management, Nov. vol2, no 5, , pp. 197-201. Netherlands.

Igbaria, Magid, Zinatelli, Nancy, Cragg, Paul, Cavaye, L.M. Angele. September 1997. "Personal Computing Acceptance factors in small firms: A Structural Equation Model," *MIS Quarterly*, pp. 279-305.

Igbaria, Magid. Greenhaus, Jeffrey H. " Determinants of MIS employees' turnover intentions: A Structural Equation Model". Communications of the ACM, Feb. 1992, vol 35, no 2, pp. 35-49.

Iglehart, K. John, Jan/Feb 1998. "The media as messenger", *Health Affairs*, 17(1), pp. 7-8.

Karen, Ignagni. "Covering a breaking revolution: The media and managed care", *Health Affairs* 17(1), 1998 Jan/Feb, pp. 26-34.

Klopfer, H. Peter, Rubenstein, Daniel. 1977. The concept privacy and its biological basis", *Journal of Social Issues*, 33(3), pp. 52-65.

Laufer, S. Robert, Wolfe, Maxine. 1997. "Privacy as a concept and a social issue: A multidimensional development theory", *Journal of Social Issues*, 33(3), pp.22-42.

Nunnally, J.C. 1978. Psychometric Theory, 2nd ed., McGraw-Hill, New York.

Orring, R. and Vainio-Larsson A. 1990. "Evaluating the usability of user interfaces: research in practice." Human-Computer Interaction. INTERACT '90. Proceeding of the IFIP TC 13 Third Conference. North-Holland. 1990, pp.323-8. Amsterdam, Netherlands.

Pearson, D. 2002. "Distribution reliability assessment. Distribution power system reliability data collection." IEEE Power Engineering Society Summer Meeting (Cat. No.02CH37376). IEEE. Part vol.2, pp. 788.

Simpson, L. Roy. July 1994. "Ensuring patient data, privacy, confidentiality and security", *Nursing Management*, 25(7), pp. 18-20.

Smith, H. Jeff, Milberg, J. Sandra, Burke J. Sandra. June 1996. "Information Privacy: Measuring Individuals' Concerns about organizational practices," *MIS Quarterly*, pp. 167-196.

Smiley, Leiott, Andsager, Julie. Summer 1998. "Evaluating the public information: Shaping ews coverage of the silicone implant controversy." Public Relations Review, vol 24, issue 2, pp. 183-201.

Solem, O. Dec 2003. Systematic Practice & Action Research. Kluwer/Plenum Publisher, Netherlands. vol 16, no.6, pp. 437-54.

Tyler, J.L. 2001 "The healthcare information technology context: a framework for viewing legal aspects of telemedicine and teleradiology." Proceeding of the 34th Annual Hawai International Conference on System Sciences. IEEE Comput. Soc. pp. 10

Warren, A. Carol, Laslett, Babara. 1977. Privacy and secrecy: A conceptual comparison, *Journal of Social Issues*, 33(3), pp. 43-51.

Warwick, Shelly. "Privacy and policy", *Bulletin of the American Society for Information Science*, 23(3), 1997 Feb/Mar, pp. 14-15.

Westin, Alan F., Cebrzynski, Gregg. Aug 16 1993. "Media access: Collision of First Amendment and privacy rules." Marketing News, vol 27 issue 17, Council for Marketing.pA17, 1/9p.
2004. http://www.healthtech.org/Common_Site/research/tfr.asp

APPENDIX I: Survey

Circle the responses using a black or a blue pen. Please do not write your name on the survey. All responses are anonymous. Thank you for your time.

Collection

1= Strongly disagree   2= Disagree to some extent   3= Uncertain   4= Agree to some extent
5= Disagree   6=Agree   7= Strongly agree

1.	It usually bothers me when companies ask me for personal medical information.	1	2	3	4	5	6	7
2.	When companies ask me for personal medical information, I sometimes think twice be fore providing it.	1	2	3	4	5	6	7
3.	It bothers me to give personal medical information to so many companies.	1	2	3	4	5	6	7
4.	I'm concerned that companies are collecting too much personal medical information about me.	1	2	3	4	5	6	7

Errors

1= Strongly disagree   2= Disagree to some extent   3= Uncertain   4= Agree to some extent
5= Disagree   6=Agree   7= Strongly agree

1.	All the patient medical information in computer databases should be double-checked for accuracy-- no matter how much this cost.	1	2	3	4	5	6	7
2.	Companies should take more steps to make sure that the patient medical information in their files is accurate.	1	2	3	4	5	6	7
3.	Companies should have better procedures to correct errors in patient medical information.	1	2	3	4	5	6	7
4.	Companies should devote more time and effort to verify the accuracy of the patient medical information in their databases.	1	2	3	4	5	6	7

Unauthorized Secondary use

1= Strongly disagree   2= Disagree to some extent   3= Uncertain   4= Agree to some extent
5= Disagree   6=Agree   7= Strongly agree

1.	Companies should not use patient medical information for any other purpose unless it has been authorized by the patients who provided the information.	1	2	3	4	5	6	7
2.	When people give personal medical information to a company for some reason, the company should never use the information for any other reason.	1	2	3	4	5	6	7
3.	Companies should never sell the personal medical information in their computer databases to other companies.	1	2	3	4	5	6	7
4.	Companies should never share patient medical information with other companies unless it has been authorized by the patients who provided the information.	1	2	3	4	5	6	7

Improper Access

1= Strongly disagree   2= Disagree to some extent   3= Uncertain   4= Agree to some extent
5= Disagree   6=Agree   7= Strongly agree

1.	Companies should devote more time and effort to preventing unauthorized access to patient medical information.	1	2	3	4	5	6	7
2.	Computer databases that contain patient medical information should be protected from unauthorized access--no matter how much it costs.	1	2	3	4	5	6	7
3.	Companies should take more steps to make sure that unauthorized people cannot access patient medical information in their computers.	1	2	3	4	5	6	7

Previous personal experience

1= never   2= to a very little extent   3= To a little extent   4= to some extent
5= to a great extent   6= extreme extent   7= to very great extent

How often have you personally been the victim of what you felt was an improper invasion of privacy?	1	2	3	4	5	6	7

Media

1= never   2= to a very little extent   3= To a little extent   4= to some extent
5= to a great extent   6= extreme extent   7= to very great extent

How much have you heard or read during the last year about the use and potential misuse of computerized information about patient?	1	2	3	4	5	6	7

Appendix II

Table 1. Assessment of the Measurement Model

Variables	The Composite Reliability (Internal Consistency Reliability)	Average Variance Extracted/Explained
Privacy Concern:		

Collection	.909	2.50
Errors	.932	2.45
Unauthorized	.941	1.30
secondary use	.907	1.60
Improper access		

Cronbach's Alpha .909

Table 2. Intracorrelation Among Variables

Variables	1	2	3	4	5	6
1. Collection	.78					
2. Errors	.30	.82				
3. Unauthorized Secondary Use	.32	.56	.87			
4. Improper Access	.33	.66	.77	.86		
5. Previous Experience	.16	.27	.11	.07	1.0	
6. Media	.17	-.05	.08	.06	.47	1.0

Table 3: Inter-Item Correlation Matrix

	Col I1	Col I2	Col I3	CO II4	Err 1	Err 2	Err 3	Err 4	UnSec U1	UnSec U2	UnSec U3	UnSec U4	IMPRP A1	IMPRP A2	IMPRP A3	Pprexl	Med
Coll1	1.000	.702	.714	.730	.270	.165	.224	.304	.164	.256	.187	.184	.255	.263	.251	.382	.166
Col2	.702	1.000	.719	.754	.180	.178	.306	.320	.238	.283	.275	.320	.255	.205	.263	.361	.161
Coll3	.714	.719	1.000	.758	.352	.371	.465	.475	.265	.348	.290	.265	.406	.433	.405	.680	.216
COII4	.730	.754	.758	1.000	.375	.295	.407	.435	.264	.344	.273	.264	.353	.374	.415	.380	.125
Err1	.270	.180	.352	.375	1.000	.806	.783	.738	.453	.396	.375	.396	.518	.695	.338	.199	.143
Err2	.165	.178	.371	.295	.806	1.000	.783	.803	.569	.536	.487	.588	.621	.380	.205	.125
Err3	.224	.306	.465	.407	.783	.783	1.000	.833	.569	.476	.547	.663	.573	.548	.518	.220
Err4	.304	.320	.475	.435	.738	.803	.833	1.000	.547	.478	.619	.473	.419	.473	.316	.229
UnSec U1	.164	.238	.265	.264	.453	.596	.569	.547	1.000	.794	.843	.781	.547	.641	.635	.617	.273
UnSec U2	.256	.283	.348	.344	.396	.536	.476	.478	.794	1.000	.763	.679	.433	.855	.633	.751	.466
UnSec U3	.187	.275	.290	.273	.375	.487	.547	.619	.843	.763	1.000	.686	.898	.719	.717	.818	.246
UnSec U4	.184	.320	.265	.264	.396	.588	.663	.473	.781	.679	.926	1.000	.717	.771	.538	.527	.370
IMPRP A1	.255	.255	.406	.353	.518	.588	.663	.619	.781	.633	.798	.771	1.000	.262	.517	.411	.066
IMPRP A2	.263	.205	.433	.374	.695	.621	.573	.473	.547	.855	.593	.388	.260	1.000	.939	.540	.000

IMPRPA3	.351	.280	.415	.436	.538	.618	.591	.580	.746	.645	.771	.701	.851	.793	1.0000	.115	.057
Pprex1	.182	.216	.138	.099	.017	.098	.020	.016	.127	.125	.081	.089	.041	.054	.115	1.0000	.466
Med1	.166	.176	.205	.143	-.129	-.073	-.066	-.029	.048	.037	.124	.099	.106	-.008	.057	.466	1.0000

The covariance matrix is calculated and used in the analysis.

APPENDIX III: Figure 1: Measurement Model
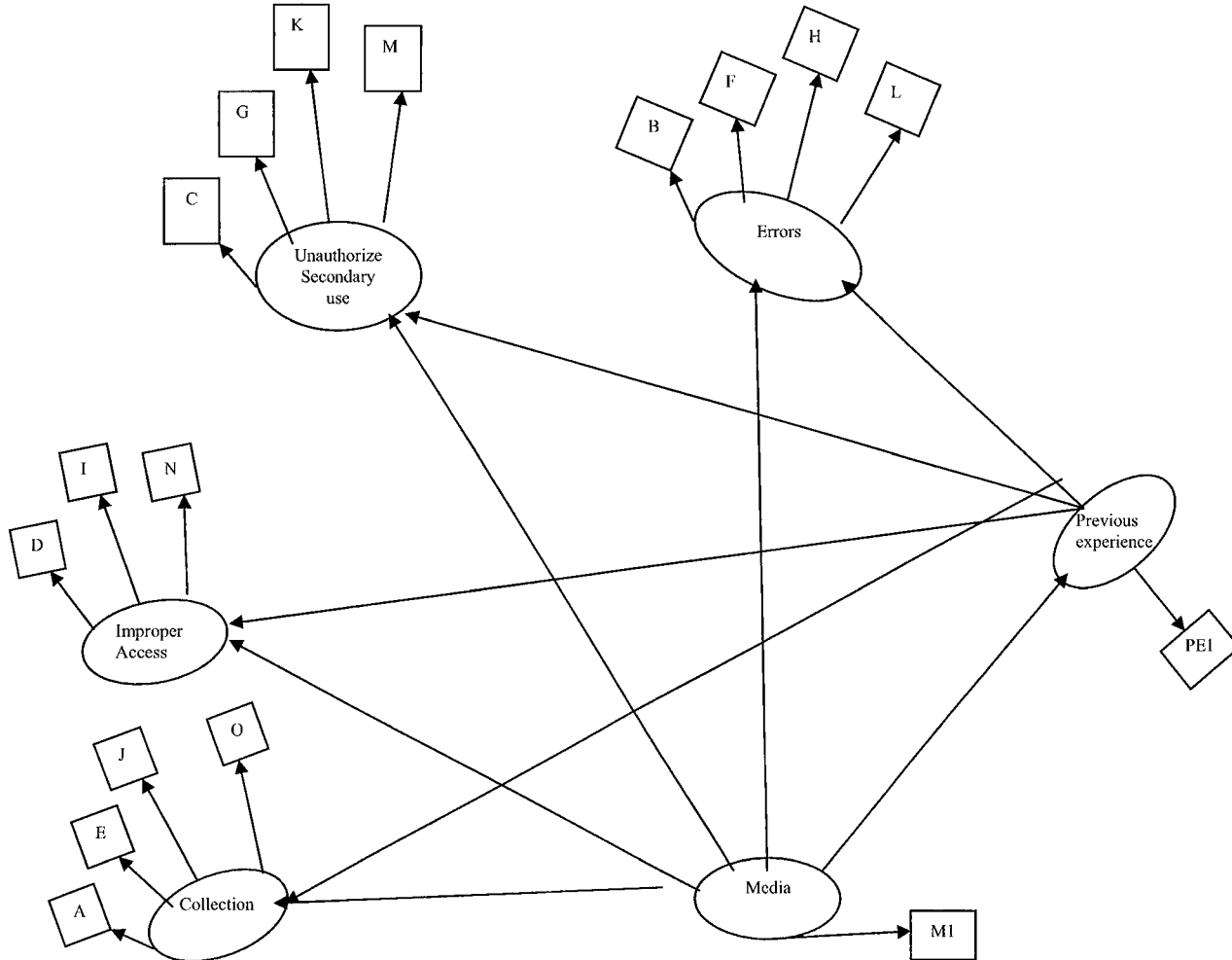
APPENDIX III

Figure 2. The Model : Factors effecting privacy concerns