8-2020

Physicians' Perceived Threats and Electronic Medical Record Workaround

Joseph A. Manga
The University of Texas Rio Grande Valley

Nan Xiao
The University of Texas Rio Grande Valley

Aug 10th, 12:00 AM

Physicians' Perceived Threats and Electronic Medical Record Workaround

Joseph Manga
University of Texas Rio Grande Valley, joseph.manga01@utrgv.edu

Nan Xiao
University of Texas Rio Grande Valley, nan.xiao@utrgv.edu

Physicians' Perceived Threats and Electronic Medical Record Workaround

Emergent Research Forum (ERF)

Joseph Manga
University of Texas Rio Grande Valley
joseph.manga01@utrgv.edu

Nan Xiao
University of Texas Rio Grande Valley
nan.xiao@utrgv.edu

Abstract

Electronic medical record (EMR) systems can improve patient care and their usages are mandatory in many health care organizations. Yet, some physicians engaged in workaround behaviors as a response to their negative experiences in using EMR. Leveraging protection motivation theory, we propose a theoretical framework to understand what causes physicians to use EMR systems less effectively. We posit that EMR systems' usability and physicians' technology capability affect their appraisal of threats associated with EMR use, which in turn influences their workaround behaviors. We conclude with some implications to research and practice, and opportunities for future research.

Keywords

Workaround, perceived threats, electronic medical records (EMR) systems.

Introduction

Electronic medical record (EMR) systems have the potential to improve patient care efficiency and productivity (Lee et al., 2010), quality of care (IOM, 2001), and reduce medical errors (Aron at al., 2011). However, such a potential may not be realized if EMR systems are not used effectively and faithfully (e.g., Beaudry & Pinsonneault, 2005). Particularly, although the use of EMR systems is mandatory in some countries such as U.S., if physicians face difficulties during their use of EMR systems, they may engage in workaround behaviors, including using the systems less often than they should or delegate the use to others altogether. Workaround (e.g., Alter, 2014) is potentially hazardous because it threatens patient privacy, employee compliance, and it affects the value and adoption of health IT (HIT). Thus, investigation of the drivers of EMR workaround is merited.

This current study leverages protection motivation theory (PMT) suggest that workaround behaviors are influenced by users' perception of threats triggered by their lack of capability to use the system and the system's limitations of possessing attributes that facilitate ease of use. PMT assumes some mechanisms of fear appeal: the magnitude of a threat, the likelihood of its happening, and efficacy of a protective response (Rogers, 1975; Chen et al., 2019). We investigate how physicians evaluate threats posed by the implementation of the HIT and how these threats impact workaround. Our research questions (RQ) are: *1. How do physicians perceive the threats associated with electronic medical record system use? 2. What factors influence physicians' risk perceptions? 3. How do physicians react to these perceived threats?*

Theoretical Background

When users of EMR systems assess their capabilities to be adequate and the systems' features to be useful and easy to use, they will interact with the system in a prescribed manner (Fernie & Metcalf, 1998). However, when users think that they do not possess the necessary skills and abilities or that the systems functionalities are somewhat difficult, they tend to resist their usages (e.g., Marakas & Hornik, 1996). Yet, a class of lukewarm users exist who are neither cold nor hot towards systems use; they do not resist nor oppose EMR use but simply display workaround behaviors. *Workaround* is defined as "*non-compliant user behaviors vis-a-vis the intended system design, which may go so far as to bypass the formal systems*

entirely" (Koopman & Hoffman, 2003, p. 264). An example of workaround includes physicians relying on handwritten patient information among themselves instead of looking it up in the EMR system because the EMR response time is slow and access to patient information is difficult. Difficulty in accessing patient information for decision making and HIT usability challenges have been documented as common factors that have contributed to workaround behaviors for healthcare professionals to adapt to changing workflows in care delivery (Gephart et al., 2015). Workarounds occur when information, technologies, and tasks interact together (Burns et al., 2015). Prior study has shown that workaround behaviors can be costly for the organization because of the time expended by employees not following the right procedure in performing their daily job (Petrides et al., 2004). Workaround behaviors may also raise compliance issues, which tarnish the image of the company, and if the behaviors persist, it may attract litigations (Rushton & Stutzer, 2015). Furthermore, engaging in workaround behaviors may cause sneaky destruction of the integrity and harm to an individual's professional career (Rushton & Stutzer, 2015). We leverage protection motivation theory (PMT) and Lapointe and Rivard's (2005) framework on IS resistance to examine physician's workaround behaviors with EMR systems implementation.

PMT explains the cognitive process of behavioral change using threat and coping appraisals. It proposes four beliefs that affect one's motivation to protect himself from danger including perceived severity—the magnitude of harm of a threat, perceived susceptibility—likelihood that a threat might occur, self-efficacy—confidence in one's ability to overcome a threat, and response efficacy—the effectiveness of recommended behaviors (e.g. support or training) in overcoming the threat (Rogers, 1975). Individuals can assess the level of seriousness of the threat and decide to react if the situation threatens their autonomy. PMT model suggests that a user's IT threat avoidance behavior is determined by perceived threat (Liang & Xue, 2010). In this study context, physicians' use of EMR systems can be limited by perceived threats that could arise from the technology features not friendly enough to ease usage or from physicians' fears and stresses due to their low drive towards technology use (Marakas & Hornik, 1996).

Lapointe and Rivard (2005) proposed that when a new information system is introduced, an initial condition interacts with an object of resistance producing a perceived threat, which then influences user behaviors. The object of resistance can be the system's specific features (e.g. user interface) and how it meets user needs and expectations (initial conditions), which are significant in changing the work and power structure within the organization or users and implementers of a system (Selander et al., 2012). The initial condition, perceived threat, and resistance behavior of the framework are captured in our model in the next section.

Model and Hypotheses

As shown in Figure 1, building on Lapointe and Rivard (2005)'s framework and protection motivation theory, we propose that technology usability affects both perceived threat severity and perceived threat susceptibility, and user capability has an impact on self-efficacy and response efficacy, which in turn influence user workaround to EMR system.

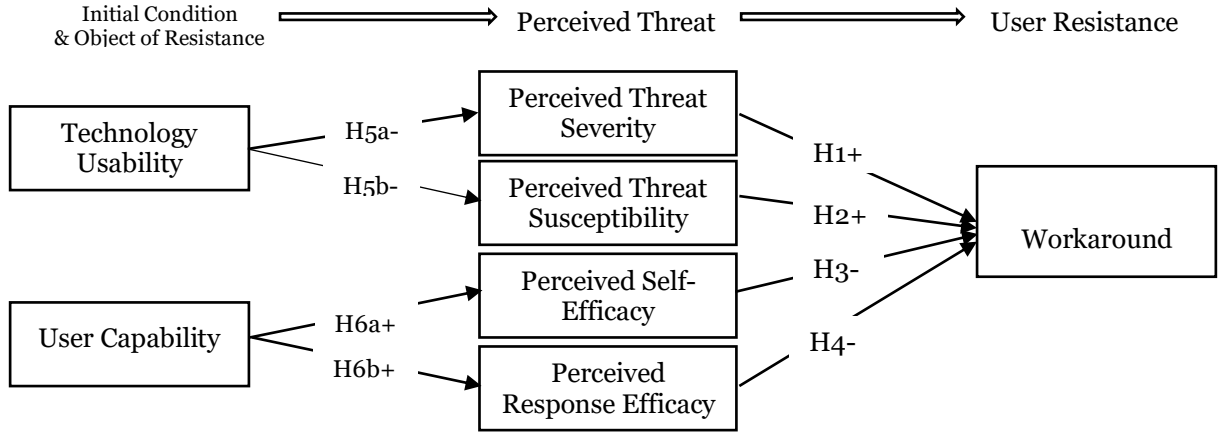

Figure 1: Conceptual Model

Perceived Threat Severity

Perceived threat severity refers to the extent to which individuals feel negative consequences in using a system. Examples of negative consequences include stress, fear, excessive workload, loss of productivity, limited time. Due to their heavy workload, physicians may have to split the limited time between face-to-face interaction with the patients and using the EMR system concurrently. If physicians feel the system use as time consuming, which negatively affects their doctor-patients relationship or sacrifice patient care quality and productivity (Loomis et al., 2011; Pont, 2000), they limit usage or delegate it to their assistants.

H1: Perceived threat severity is positively associated with EMR system workaround.

Perceived Threat Susceptibility

Perceived threat susceptibility is defined as the likelihood that an individual will experience the negative consequences associated with the use of a system. Negative consequences can increase the risk of system use. Physicians minimize the risk by engaging in workaround. The probability of a suspected threat is subjective and perceived probability of negative consequences give rise to threat perceptions (Liang & Xue, 2010). If physicians have strong beliefs that these consequences will happen and affect them negatively, then they will be more cautious and hence, find alternative ways to use systems. "Once an individual is aware of a threat, he or she will establish beliefs about the probability of experiencing it," (Johnston & Warkentin, 2010, p. 551). However, physicians will perceive systems as less threatening if the consequences are less likely to happen. Perceived susceptibility increases the negative consequences of the threat (Liang & Xue, 2010). Thus, physicians will work around a system when susceptibility is high. So,

H2: Perceived threat susceptibility is positively associated with EMR system workaround.

Perceived Self-Efficacy

Perceived self-efficacy refers to the extent to which a user believes he or she is confident in his/her ability to overcome threats to system use and implementation. EMR systems' features can challenge users' ability to interact with systems effectively. For example, learning to use a new system requires time and efforts, which could lower a physician's overall work performance (Davis et al., 1989). Also, a physician's fear and stress level can threaten his confidence to navigate a system (Johnston & Warkentin, 2010). When physicians perceive their confidence to be low, it affects their self-efficacy negatively and thus, influences their use of the system, thereby encouraging workaround. When individuals have low confidence, poor abilities, and low self-efficacy (Bandura, 1994), they will look for other means of doing things. Thus, users low in self-efficacy will practice more workaround than higher self-efficacy individuals.

H3: Self-efficacy is negatively associated with EMR system workaround.

Perceived Response Efficacy

Perceived response efficacy refers to the degree to which users believe they can effectively use support or training to help them overcome the negative consequences of threat. Physicians may receive various supports and training (S&T) from management, colleagues, IT department (via casual interactions or formal face-to-face or online training programs) to overcome the negative consequences of perceived threats. When an individual's control over the use of a system is disrupted, he/she may take actions by seeking help. If the physician's concerns can be addressed in the training, they are more likely to accept the system and will continue to use it properly (Beaudry & Pinsonneault, 2005). Additionally, adequate training can increase the understanding of system's features and functions, facilitating physicians' use of the system. Studies showed that management support for change reduces usage misbehaviors (Kim & Kankanhalli, 2009). If physicians feel that S&T are sufficient, then they will not workaround, otherwise they will.

H4: Response efficacy is negatively associated with EMR system workaround.

Technology Usability

Technology usability refers to the degree to which an electronic medical record (EMR) system can be easily used or learned without excessive efforts. A technology's usage is determined by behavioral intention

to use it, influenced by the perceived usefulness (Davis et al., 1989). The EMR system needs to accomplish the purpose it was built for to be considered useful. When a system provides all the necessary functionalities to ease usage and performs with accuracy and speed, then it will not be seen as threatening and any perceived threat will be inconsequential. However, if the system causes physicians to spend a greater percentage of their work time figuring out how to navigate it or trying to find out where to pull up patients' information, it arouses their perceptions of system complexity and difficulty, and perceived threats will be considered serious and harmful. Therefore, physicians' perceptions of an ineffective and inefficient system will signal the seriousness of the threat, increase the perceived threat, and reveal the severity of the threat. Thus, a technology's complexity and difficulty increases threat severity. Hence,

H5a: Technology usability is negatively associated with perceived threat severity.

Physicians' perceptions of an ineffective and inefficient system will also signal a likelihood/susceptibility of the threat and a system's perceived difficulty and complexity create an awareness that a threat exists. Once users are conscious of a threat, they form beliefs about the likelihood of experiencing it (Johnston et al., 2015). If the system design does not address users' needs, it may introduce perceptions that the system is more likely to be faulty, problematic, inefficient, and ineffective. Therefore, we hypothesize that:

H5b: Technology usability is negatively associated with perceived threat susceptibility.

User Capability

User capability refers to the degree to which individuals believe they possess the skills and knowledge required to use a system effectively. IT-related skills, knowledge about workflow, and ability to learn new things could influence user's confidence and response to system use. The more skills a physician has, the more likely they will be confident. Mastery experiences provide skills that rely on successes to build one's belief in self-efficacy (Bandura, 1994), but failures could threaten an individual's self-efficacy. When physicians' experience with a system is so easy, they tend to be less resilient in their efforts to master and overcome the challenges of using it. Any difficulty in the system will limit their ability to take actions to avoid the threat. So, physicians who demonstrate higher capabilities will be more confident in themselves and will be able to overcome system threats. However, if physicians who are not assertive of their abilities will be less motivated to learn and their confidence level will plummet, leading to low self-efficacy. Thus:

H6a: A user's capability is positively associated with his/her perceived self-efficacy.

User capability will also increase the perceived effectiveness of S&T to overcome negative consequences. A lack in a physician's IT skills and unfamiliarity with the system's interface will lower their confidence (Loomis et al., 2002) in the S&T they receive. Physicians who do not believe they possess the skills and knowledge necessary to understand the training content or articulate their needs for help, may feel the S&T will be of little help to them. However, physicians with high degrees of IT-related skills will see S&T as an added advantage to assist them curb the threatening and adverse consequence to system use. Thus,

H6b: A user's capability is positively associated with his/her perceived response efficacy.

Conclusion and Further Work

This study contributes to research by integrating Lapointe and Rivard (2005)'s framework and Protection Motivation Theory (PMT) to understand workaround behaviors and how appraisal and coping mechanisms of PMT affect physician workaround. We also looked at the perceived threats encountered by physicians via the lens of PMT, something that has not been examined in previous studies. From now until the AMCIS conference, our major focus is designing the measurement scales and metrics and collecting data via surveys. Metrics for user resistance will be adapted from IT avoidance literature (Lapointe & Rivard, 2005), technology usability and user capability scales will be adapted from PMT literature, and perceived severity, perceived susceptibility, perceived self-efficacy, and perceived response efficacy scales will be adapted from PMT literature (Liang & Xue, 2010). We plan to survey residents and fellows (around 200 physicians) in the medical school of our university regarding their EMR use. When testing the model, we will add control variables such as a physician's workload and specialty. We will also explore alternative paths in the models such as the direct relationships between technology usability/user capability and workaround as well as whether the mediation is a full or partial one.

References

Alter, S. 2014. "Theory of workarounds," *Communications of the Association for Information Systems*, 34, pp. 1041-1066.

Aron, R., Dutta, S., Janakiraman, R., & Pathak, P. A. 2011. "The impact of automation of systems on medical errors: evidence from field research," *Information systems research*, (22:3), pp. 429-446.

Bandura, A. 1994. "Self-efficacy," In V. S. Ramachaudran (Ed.), *Encyclopedia of Human Behavior*, 4, pp. 71-81. New York: Academic Press.

Beaudry, A., and Pinsonneault, A. 2005. "Understanding User Responses to Information Technology: A Coping Model of User Adaptation," *MIS Quarterly*, (29:3), pp. 493-524.

Burns, A. J., Young, J., Roberts, T., Courtney, J. F., & Ellis, T. S. 2015. "Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective," *AIS Transactions on HCI*, (*7*:3), pp. 142–165.

Chen, C., Zhang, K. Z., Gong, X., Lee, M. K., & Wang, Y. 2019. "Decreasing the problematic use of an information system: An empirical investigation of smartphone game players," *Information Systems Journal*, pp. 1-43.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, (35:8), pp. 982-1003.

Fernie, S., & Metcalf, D. 1998. *"(Not) hanging on the telephone: payment systems in the new sweatshops (No. 390),"* Centre for Economic Performance, London School of Economics and Political Science.

Gephart, S., Carrington, J. M., & Finley, B. 2015. "A systematic review of nurses' experiences with unintended consequences when using the electronic health record," *Nursing Administration Quarterly*, (39:4), pp. 345–356.

Institute of Medicine (IOM). 2001. "Crossing the Quality Chasm: A New Health System for the 21st Century," *National Academy Press*, Washington, DC.

Johnston, A. C., & Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, (34:3), pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly*, (39:1), pp. 113-134.

Kim, H-W., & Kankanhalli, A. 2009. "Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective," *MIS Quarterly* (33:3), pp. 567-582.

Koopman, P., & Hoffman, R. R. 2003. "Workarounds, make-work, and kludges," *IEEE Intelligent Systems*, (*18*:6), pp. 70–75.

Lapointe, L., & Rivard, S. 2005. "A Multilevel Model of Resistance to Information Technology Implementation," *MIS Quarterly*, (29:3), pp. 461-491.

Lee, J., McCulloug, J., & Town, R. 2010. "The Impact of Health IT on Hospital Productivity," Working paper, University of Minnesota, Minneapolis.

Liang, H., & Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, (11:7), pp. 394-413.

Loomis, G. A., Ries, J. S., Saywell, R. M., & Thakker, N. R. 2002. "If Electronic Medical Records are so Great, why aren't Family Physicians Using Them?" *Journal of Family Practice* (51:7), pp. 636-641.

Marakas, G. M., & Hornik, S. 1996. "Passive Resistance Misuse: Overt Support and Covert Recalcitrance in IS Implementation," *European Journal of Information Systems*, (5:3), pp. 208-220.

Petrides, L. A., McClelland, S. I., & Nodine, T. R. 2004. Costs and benefits of the workaround: inventive solution or costly alternative. *Int'l Journal of Educational Management*, (18:2), pp. 100–108.

Pont, E. A. 2000. "The Culture of Physician Autonomy: 1900 to Present," *Cambridge Quart. Healthcare Ethics*, (9:1), pp. 98–113.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology*, (91:1), pp. 93–114.

Rushton, C. H., & Stutzer, K. 2015. "Ethical Implications of Workarounds in Critical Care," *AACN Advanced Critical Care*, (26:4), pp. 372–375.

Selander, L., & Henfridsson, O. 2012. "Cynicism as User Resistance in IT Implementation," *Information Systems Journal*, (22:4), pp. 289–312.