# Healthcare Professionals' Views on Security – A Text Analytical Approach

*Emergent Research Forum Paper*

**Xiaoni Zhang**
Northern Kentucky University
zhangx@nku.edu

**Vijay Raghavan**
Northern Kentucky University
raghavan@nku.edu

## Abstract

Technological advancement has revolutionized patient care. With massive amount of data collected patients, personalized treatment can be provided. However, technology is a double-edge sword. Both news and media report the significant impact of security breaches, study of security is needed and as our work, life and health continually rely on more technologies, any breach or failure of the system could create disastrous impact. In this paper, we use a text analytic approach to study healthcare professionals' view on security. Data were collected from 50 healthcare professionals with an average work experience of 17.5 years. A total of 145 posts were analyzed. The results indicate that healthcare organizations need to invest on employee training on security, developing standards in healthcare terminologies as well as security and privacy policies related to mobile and social media use.

**Keywords**

Healthcare, security, text analytics

## Introduction

Technological advancement has revolutionized patient care. With massive amount of data collected on cancer patients, personalized cancer treatment can be provided (Edward, 2014). However, such advancement does not come without difficulties. Healthcare's digital transformation has put health records at greater risk (Millerman 2014). News of security breaches include nationally recognized insurance companies, pharmacies, and community health care offices. Recently, Federal authorities investigate a virus that infected all of the electronic services among the Appalachian Regional Healthcare (ARH) System in Kentucky and West Virginia. All ARH system computers were shut down to prevent the further spread of the virus. Consequently, medications, patient-care, registration, imaging, and laboratory services are being coordinated manually (Virus affects AHR", 2016).

Health care data accounted for 43 percent of major data breaches reported in 2013 (Identity Theft Resource Center). Both news and media report the significant impact of security breaches, study of security is needed and as our work, life and health continually rely on more technologies, any breach or failure of the system could create disastrous impact. What are the issues related to security? How to address these issues? What are the insights when performing text analytics on views/opinions expressed by healthcare professionals?

To answer these questions, this paper focuses on how we might extract security information and knowledge from healthcare professionals. We also contribute to the literature on security and healthcare domains Specifically, this paper uses text analytical approach to explore the views expressed by the healthcare professionals. In so doing, this paper provides a survey of the literature on security in healthcare, and this paper contributes to the literature in the following: 1) survey the literature on security in healthcare; 2) perform text analytics on the views provided by healthcare professionals; 3) provide implications of the results.

# Background

## *Security*

Security is concerned with protecting confidentiality and the integrity of data (Baker, 2015). Security breaches can be a result of several underlying issues such as unintended disclosure (sensitive information mishandled or sent to the wrong party), hacking or malware (electronic entry by an outside party), insider (someone with legitimate access leaks information), lost or stolen devices with access to information (Privacy Rights Clearinghouse). Creating secure applications is more than ever a complex task because it requires system engineers with increasing levels of knowledge in security requirements, design and implementation (Ruit et al., 2017). Information security risks are often interdependent and thus may cause firms to invest inefficiently in information technology security management. Zhao et al. (2013) propose two risk management approaches and suggest cyberinsurance is a promising solution to help firms optimize security spending.

## *Healthcare Security*

In healthcare, electronic health records (EHR) has been widely implemented. EHR is essential to collect patients and treatment related information and provide safe, effective patient care. EHR enables a new era in the continuity of care by allowing providers and facilities immediate access to patient and administrative information for decision making. Through these systems, patient information is monitored, as well as the quality of care and evaluation of outcomes (Saba & McCormick, 2011). However, cloud computing, wireless health devices and sensors, and poorly encrypted healthcare data remain vulnerable to security and privacy issues. For example, a group of hackers compromises the EMRs in hospitals owned by Community Health Systems (Amons, 2014). WSMV-TV in Nashville reported that patient's personally-identifiable information (such as dates of birth and social security numbers) was stolen, luckily, the actual diagnosis or treatment information was not accessed. Lack of privacy and security enhance patient information to be vulnerable and increase the risk of a cyber-attack (Health IT.gov, 2016).

# Method

In this paper, we intend to identify healthcare professionals' views on security. Given our research questions, using a qualitative method is appropriate. To make our analysis methods more rigorous, we used two methods to explore data – content analysis to manually analyze themes and SAS Text Miner to automate the analysis process. We present the results of the content analysis in this paper and hope to present the results of SAS Text Miner at the AMCIS conference in August.

# Data Collection

Data were collected from students enrolled in the graduate Health Informatics Program and students in the Doctoral of Nursing Practice program between Spring 2015 and Fall 2016. Students in the Doctoral of Nursing Practice had an average of 21.5 years patient care experience and students in the Health Informatics program had an average of 10.7 healthcare experience. The participants can be classified into medical (nurses) and non-medical professionals (trainer, administrators etc.).

As part of course requirements, students were asked to participate in the online discussion of security in healthcare on Blackboard. The discussion thread was titled "Discuss security issues in healthcare." The discussion thread was open to students for a week. During this period students posted, reposted and commented on others' posts. To eliminate confounding effect, the instructor was not participated in any of the discussions. The purpose was to encourage students to interact with each other. A total of 145 posts made by 50 students were collected. There were 24 doctoral students and 26 graduate students participated in the online discussion forums.

## Data Analysis

Blackboard posts were copied to a word file and each post was carefully analyzed to develop central themes. Themes, the length of each post, author's specific information (demographic variables) were saved in an SAS table to prepare for later text mining. Next, based on the central ideas, categories and sub-categories were developed. Several iterations of fine-tuning categories were conducted until we deemed that theme saturation has been reached.

## Results

The following describe themes developed from the posts.

### *Process Issue*

Process control is critical. Anything computer-based goes back to "GIGO"-Garbage in, garbage out. When charting patients, dual diligence must be exercised. Giving patient' charts an extra once-over is a good practice before electronically signing them. In addition, duplicating procedures is another problems.

> *"I am embarrassed to say that I've several instances in which I began to give test results to the wrong patient because of a misfiling of test results in someone else's chart."*

### Standardization

Standardization is lacking in healthcare. As indicated by five participants, they feel that standards should be developed to build a single version of the truth.

> "*I firmly believe that standards need to put in place by the health informatics community for vocabulary, collection, storage, analysis, integration, ownership, dissemination, and privacy. In order to advance the evidence base in medicine, we need standards to facilitate efficient and effective data mining."*

### *User Issue*

Employee training is critical. Careless employees expose an organization to security risks. Though they receive training on privacy and computer use security, they may not follow the security protocols at workplace.

> *"Often patient charts being pulled up on the computer and then left open is something that I have seen as well. We have been reminding others to log off. It can be a violation of patient privacy."*

### *Social Media*

Social media is another outlet for privacy invasion. Some employees post selfies in the workplace on Facebook and Instagram. Security policies on social media are still under development and the policies vary from state to state and organization to organization (Shrift 2015).

> *"We are struggling with the social media policy on many levels and whether staff should be able to make comments or post pictures from work at all. My advice to young nurses is that work and work-related feelings and emotions do not belong on social media - period. Find another outlet because the line for whether you violate someone else's privacy is thin."*

### *Reliability*

Reliability can be an issue in healthcare data collection especially when numerous people are collecting the data. Three participates told a story their bad experience with data. They ran into the situation like data was incorrectly entered. The other had issues with treatment. It seemed that doctors do not review prior treatment nodes before subscribing another set of radiological order.

> *"If I run a report at two different occasions and get different results, this might impact the care provided, which results in suboptimal or potentially dangerous outcomes. I have also run reports in systems where I get 2 different sets of values when running the same report on the same day. For reliable data, users must make sure they understand the parameters, settings, definitions, and results in order to make sure data is reliable."*

### *Interoperability*

Systems at hospitals and physician offices lack interoperability resulting the inability to merge and transfer data between different systems. This barrier of interoperability is of great concern as few electronic records systems allow for an exchange of clinical data between hospitals or from hospitals to physician's offices. Such barrier also undermines the potential value of EHR systems, causing failure to meet providers' expectations and improve patient outcomes (Jha et al., 2009).

## Conclusion

Technological innovation may be the single most powerful influence on the future of healthcare. It has shaped the conversation about the meaning of competent, timely, efficient care, the delivery of care, who owns the record of the care and how the record is accessed, managed, utilized and protected, etc. Security, privacy and reliability are three important areas in healthcare, all of which are separate but related in some ways. Legislatures are lagging behind technological advancement. Even though breeches are covered by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act (HIPAA), they certainly still occur, even on a large scale as seen in recent national media. It is imperative that heathcare organizations invest resources on employee training, security assessment, and security audit on a regular basis day-to-day to better protect patients' information.

## REFERENCES


Ahmad, R., Samy, G.N., and Smail, Z. 2010. "Security Threats Categories in Healthcare Information Systems," *Health Informatics Journal* (16:3), pp. 201-209.

Baker, D. B. 2015. Trustworthy systems for safe and private healthcare. In In V. K. Saba & K. A. McCormick (Eds.), Essentials of nursing. *Informatics*, (6th ed., pp. 145-160). New York, NY: McGraw- Hill Education.

Berner, Eta S., Sandhu, A. S., and Goodman, K. W. 2005. "Consumer health informatics: ethics, evaluation and standards." *Acta Bioethica* (11.2), p. 133.

Birnbaum, D., Elizabeth Borycki , Bryant Thomas Karras , Elizabeth Denham , Paulette Lacroix. "Addressing Public Health informatics patient privacy concerns", Clinical Governance: An International Journal 20.2 (2015): 91 – 100. Emerald Insight. Web. 10 Aug. 2015.

Chatterjee, S., Sarker, S., and Valacich, J. S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* (31:4), pp. 49-87.

Diana, A. 2014. When Big Data & Infants' Privacy Collide. *Information Week,* http://www.informationweek.com/healthcare/security-and-privacy/when-big-data-and-infants-privacy-collide/d/d-id/1306616? Retrieved Feb. 22, 2017.

Edwards, C. 2014. Using patient data for personalized cancer treatments. *Communications of the ACM* (57:4), pp. 13-15.

Free, J. 2014. "Real-world BYOD Security BYOD Security Strategies from Two Distinct Healthcare Organizations," *Health Management Technology* (35:3), pp. 14-17.

Goreva, N., Mishra, S., Draus, P., Caputo, D. 2016. "Impacts of Organizational Structure and Business Processes on Effective Security Governance in Healthcare Organizations," in Proceedings for the Northeast Region Decision Sciences Institute (NEDSI), pp. 1-12.

Health IT.gov. (2016, February 12). Privacy & Security. Retrieved from Health IT. gov: https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources, accessed Feb. 23, 2017.

Identity Theft Resource Center. "ITRC 2013 Breach List Tops 600 in 2013," http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html, accessed Feb. 20, 2017.

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., ... & Blumenthal, D. (2009). Use of electronic health records in US hospitals. New England Journal of Medicine, 360(16), 1628-1638. DOI: 10.1056/NEJMsa0900592.

Karamjit, K. & Rinkle, R. 2015. Managing data in healthcare information systems: Many models, one solution. *Computer*, 48, (3), 52-59.

Levine, B.A., and Goldschlag, D. 2014. "Do Healthcare Data Belong in The Cloud?" *Contemporary OB/GYN* (7), pp. 34-36.

McMillan, M. 2011. HITECH security mandates for healthcare organizations. Healthcare Financial Management

Mewborn, A. 2016. Healthcare security is a global concern. Industrial Engineer: IE.(48:11), pp. 20-20.

Millman, J. 2014. "Health care data breaches have hit 30M patients and counting," Washington Posts, https://www.washingtonpost.com/news/wonk/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/?utm_term=.44b7e1976f57, accessed Feb. 20, 2017.

Monsen, K., Lytton, A., Ferrari, S., Halder, K., Radosevich, D., Kerr, M., Mitchell, S., and Brandt , J. 2011. "Evaluating reliability of assessments in nursing documentation," *Online Journal of Nursing Informatics* (15:3). Retrieved from http://ojni.org/issues/?p=899

O'Leary, D. E. 2001. Blog mining-review and extensions: "From Each according to His Opinion," *Decision Support Systems* (51:4), pp. 821-830.

Ruiz, J. F., Arjona, M., Maña, A., Rudolph, C. (2017). "Security Knowledge Representation Artifacts for Creating Secure IT Systems," *Computers & Security* (64), pp. 69-91.

Semel, M. 2016. "Why Security and Compliance Are Executive Responsibilities," *Journal of Health Care Compliance* (18:2), pp. 17-51.

Shrift, B. (2015). Protect your assets with a social media policy. *Healthcare Business Monthly*, p. 54-55.

Taddicken, M. 2014. "The 'Privacy Paradox' in the Social Web: The impact of Privacy Concerns, Individual Characteristics, and The Perceived Social Relevance on Different Forms of Self-Disclosure," *Journal of Computer-Mediated Communication* (19:2), pp. 248-273.

Tanner, Adam, "For Sale: Your Medical Records". Scientific American, 2/1/2016, at http://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

Virus affects ARH hospitals' computers in 2 states. 2016. http://www.wave3.com/story/32862577/virus-affects-arh-hospitals-computers-in-2-states

Yarmand, M. H., Sartipi, K., Down, D. G. 2013. "Behavior-Based Access Control for Distributed Healthcare Systems," *Journal of Computer Security* (21: 1), pp. 1-39.

Zhao, X., Xue, L., Whinston, A. B. 2013. "Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements," *Journal of Management Information Systems* (30:1), pp. 123-152.

Zikos, D. 2013. Data Issues for Clinical-Administrative Decision Making in Healthcare. Phd Health Informatics. Retrieved from: https://www.researchgate.net/profile/Dimitrios_Zikos/publication/276866760_Zikos_D_Data_Issues_for_Clinical_-_Administrative_Decision_Making_in_Healthcare_Digital_Lecture_Companion/links/555aea3a08ae980ca6119390.pdf