

Privacy Issues in Healthcare

Rohit Valecha*, Jae Ung Lee*, H. R. Rao*

SUNY Buffalo

Introduction

Privacy is a basic human right (Warren and Brandeis, 1890). Privacy is the right of an individual in controlling personal information from being disclosed. Privacy is the ability to selectively share information (PCAST, 2014). With technological advances, such as cloud computing and big data, providing privacy is becoming ever-so complex.

In the healthcare domain, the emergence of patient health information management systems has transformed the healthcare model (Abraham et al. 2008). The healthcare system consists of transitive workflows with information flowing from various cross-boundary organizations (Lechler et al., 2011). In the healthcare domain, privacy is an important factor. Many of the attributes of patient health information (PHI), including condition information, treatment dates, etc., are considered private. Despite the technological advancements and workflow intricacies, there has been no comprehensive report to look at privacy in the healthcare domain. This white paper is a step towards identifying privacy issues in the healthcare domain. We identify key questions that are important for further research.

Privacy Objectives

There have been instances where the privacy of patients was compromised. Let us consider a recent scenario from Lechler et al. (2011) wherein a research facility uses a cloud vendor for storing identifiable data, personal data and medical data, and a service organization uses the same vendor for archiving

personal data and medical data. The vendor may now be able to match the patient data from the research facilities with that of service organizations, and derive more information than what is intended for the vendor. In such a case, the vendors can leak information by aggregating the data obtained from different sources. National Institute of Science and Technology (NIST) has identified this as unanticipated revelation in their recent initiative (NIST, 2014).

Furthermore, unanticipated revelation is amplified in the transitive health workflows, in which patient data flows from one organization to another. These organizations may be regulated by varying legislations from one region to the other. Valecha et al. (2012) have demonstrated this unintended disclosure using a real-world case that involves physician requesting read access to patient's diagnosis from the researcher in the laboratories. When data is exchanged between organizations, each of the agencies contributes its bits-and-pieces of patient information onto the others, resulting in a larger pool of patient information that is subject to aggregation of patient records and details. This is also commonly the case with health information exchange (HIE) systems that aim to bring patient information exchanges under a common umbrella. Examples of such revelations exist across IT solution providers that obtain data from various agencies such as insurance, labs, hospitals, etc., in order to provide data analytics to related organizations (Sokolova et al., 2009).

The unanticipated revelation can be exploited by private or online companies in negative ways, such as identity thefts, billing frauds and targeted product advertisements, to name a few. Unanticipated revelation has adverse effects on both patients (NIST, 2014) and organizations. For patients, it may result in discrimination in the society, or embarrassment at work. Fear of such discrimination may cause social and mental discomfort and inconveniences. In the long term, it may lead to ignorance for the patient to go for any treatment, ending in substantial harm to the patient. For organizations, there is loss of reputation and negative media coverage associated with such leakages and/or breaches. The

patients lose their trust within the organization to handle their data. Besides that, organizations also incur penalties ranging from thousands to even hundreds of thousands of dollars (Tanna et al., 2005). Finally, public trust in healthcare delivery system as a whole cannot be maintained if privacy rights are not addressed.

There are some major barriers to achieving privacy for safeguarding against unanticipated revelation: employee training, health technology and regulatory standards (Hersh, 2004). There is a lack of procedures for training healthcare employees on storing and handling patient information. There is no provision for identifying minimalistic information sets within information exchanges, and privacy violations associated with each of the exchanges. While in the security and safety fields, risk management models, along with technical standards and best practices, are well-developed, to date, the privacy field has lagged behind in the development of analogous components (NIST, 2014). The privacy principles (such as the Fair Information Practice Principles (FIPPs) and the Generally Accepted Practice Principles (GAPPs)) are important components of an overall privacy framework, but on their own they have not achieved consistent and measurable results in privacy protection (NIST, 2014).

Research Question: What are the critical barriers and would different contexts of health change the way barriers are perceived?

Assessment Capabilities

Healthcare systems are moving to processing health records electronically. To ensure protection of patients' information in healthcare setting, federal government issued the Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA "specifies the privacy, security and electronic transaction standards with regard to patient information for all health care providers" (Volonino & Robinson, 2004). It requires the establishment of national standards for electronic health information transactions.

To develop national standards to control the flow of sensitive health information, federal government established Privacy Rule to determine who, when and how of the access to patient information. Privacy Rule governs the regulations for creating, receiving, or maintaining such information (HIPAA, 2004). Furthermore, to ensure patients' privacy in an electronic information exchange, federal government's Fair Information Practice Principles (FIPPs) also provides guidelines for collecting and using personal information, and safeguards to assure that practice is fair and privacy preserving.

Risk management (ISO31000, 2009) is a fundamental driver of organization's approach to privacy (NIST, 2014). Privacy assessment determines the risk involved in a system or service. Assessing privacy risks can be performed through Privacy Impact Assessment (PIA, 2014). PIA focuses on identifying the effect of a task, program or technology on privacy, and mitigating the risks in the process through means of quick actions. It asks a set of questions in determining risks, and derives set of codes in reducing the risks. It can be combined with other risk management techniques to assess risk in the process of collection, storing and sharing of patient information.

A standard risk model also provides guidance on risk assessment. According to this model, risk assessment defines the nature of permitted actions, and consists of examine, interview and test methods. The examine method is the process of reviewing, inspecting and observing, studying or analyzing one or more assessment objects in order to achieve clarification. The interview method is consists of holding discussions with individuals and obtaining evidence. Finally, the test method compares the actual with expected behavior under specified conditions. Further, it allows managing risk through four methods: acceptance, transfer, mitigation and avoidance of risk.

NIST (2014) extend this standard risk model to the privacy domain by focusing on the privacy impact on individuals whose information is collected, used, stored, and transmitted by information systems. In order to understand the magnitude of privacy risk within an information system, the privacy risk model

focuses on the risk problematic data actions occurring that could result in privacy harm to individuals (Solove, 2006). It is intended to help organizations identify where controls can be most effectively implemented and facilitate proactive steps to mitigating privacy risks. It also concentrates on the data actions becoming problematic or threats which the system designer can better recognize and control.

Threat models have been popular in security domain. They provide a description of set of security aspects, and allow analysts to identify a set of possible attack points. Threat models identify assets of value, their vulnerabilities, threats that can potentially exploit these vulnerabilities, and appropriate security countermeasures to mitigate the threats. Deng et al., (2011) extended this concept to a privacy threat model. The privacy threat model instructs what issues should be investigated, and where in the model those issues could emerge, by defining a list of privacy threat types, and providing the mappings between threat types and the system elements. It allows mapping the existing privacy-enhancing technologies to the identified privacy threats.

Research Question: How do interactive threats impact health privacy and what can be the antidotes to such threats?

Multi-Disciplinary Approach

The tendency of professionals with similar backgrounds to view privacy result in overlooked perspectives, which is a well-known limitation. To overcome this limitation many professionals incorporate multiple perspectives by integrating the viewpoints of various other professionals from different domains. The combined influences of different domains help to strengthen privacy and security of healthcare information systems.

Multiple disciplines can be accommodated: security and technology professionals for developing and designing cyber protocols and techniques, economics professionals for exploring economics of personal data and its link to privacy regulations, organizational corporates for data-driven agreements, lawyers

for regulations pertaining to policies, academicians for models and methods to address privacy-preserving approaches, and federal government for setting national standards for health information exchanges. There should be initiatives for general public on privacy risk, and on consent to their data, besides training programs for theft prevention, fraud reporting, etc.

Privacy is affected by cultural dimensions (Bellman et al., 2004), which is evident from the comparison of privacy between European Union and United States. This cultural dimension determines what agency has the share of responsibility towards protecting private information. There are two regulatory models that are related to privacy: regulation model with government controlling health policy enforcement, and the self-regulation model with individuals and organizations dictating regulations (Zwick & Dholakia, 1999). In order to develop privacy in this tectonic era, it is necessary to consider shared regulations with partnership between government and other organizations in enforcing privacy policies.

Research Question: Are there potential solutions for health privacy in other cultures that can be adapted to our scenario?

Privacy Architectures

The internet privacy framework is a 'notice and consent' framework (Langheinrich, 2001), which notifies the user about its usage of their private information, and seeks consent for the same. Most of the software programs that require clicking the 'I Agree' button utilize such a framework. With the help of cookies, many websites also collect information from the user, without making them aware of the same. The terms and conditions document describes the ways in which the information will be collected, stored and shared. The user is not well equipped to understand consent notices as they are structured because it is full of legal and technical jargons.

To solve this problem, federal government established a responsible use framework (Big Data Report, 2014) for dealing with privacy. It refers to the usage of patients' private data that is available online. It

shifts the responsibility or privacy from the individual to the organizations that collect, maintain, and use data. Responsible use also holds organizations accountable for how they manage the data, rather than merely describing if the consent was properly obtained at the time of collection.

In a transitive health workflow, various organizations share patient information between them. In this process, patients' information may be divulged to outside sources without their consent. To safeguard against such practices, it is necessary to implement privacy-preserving architectures. Privacy-preservation is the process of ensuring privacy of data while completing a task, and with only minimal amount of essential information (Xiao & Tao, 2006). In this process, there is constant attempt to avoid revealing extra information by which patients' privacy may be put at stake. There are many models that enable privacy-preservation, and are investigated in data publishing, data mining, data exchange and data storing.

Most of the existing data systems focus primarily on the policies and guidelines pertaining to the nature of data available for use. However, privacy-preserving data system enables organizations to utilize the required information while maintaining privacy (Fung et al., 2010). The general objective is to transform the original data into some anonymous form to prevent from inferring its record owners' private information. For example, in order to generate data on diabetic men treated in the hospital, the administrator needs to make sure that the data is anonymized.

By incorporating privacy-preservation mechanisms in the responsible use framework, we develop the architecture for privacy risk detection and mitigation. In meeting the organizations' responsibility in collecting, maintaining, and using data, we suggest that the patient health information be masked or encrypted while at rest or in transition. In a transitive health workflow where data is sent from one organization to the other, if the data is not risk-proof, then the receiving organization faces the problem of privacy risk.

In the architecture, the organization uses the threat model to determine the risk of problematic action in the valued asset, and specify policy set to mitigate the risk. The threat is mitigated with the help of formalized privacy policies. When one organization (consumer) requests access to patient data from another organization (provider), threat model is utilized to assess the risk to the patient data. The threat model generates policies (Valecha et al., 2014) as counter-measures to the threats. The patient data is masked or encrypted using the policy set as the key, and then transferred along with policy set to the consumer organization. The policies are evaluated within the consumer system to determine whether the patient data is safe to access. If the policies detect no threat to the patient data, then it is unmasked or decrypted for the requested access.

For example, consider the scenario where a physician requests (1) read access to patient's diagnosis from the researcher in the laboratories. The researcher sets up policies (2B) that accompany the masked patient diagnosis data (2A) to the hospital side. The policy is evaluation in the actual conditions of physician mode of access, only after which the diagnosis data gets available for reading by the physician.

This is detailed in a step by step manner below:

1. Physician sends request for Value Asset to the researcher
2. Researcher utilizes threat model to identify threats and vulnerabilities of the value assets
3. Researcher also generates a policy to counter the threats
4. Researcher sends Value Asset to the physician, masked or encrypted using the policies
5. Researcher also sends policy to the physician
6. The received policy is matched at the physician end; if satisfied (meaning no threat detected), then the value asset is decrypted.

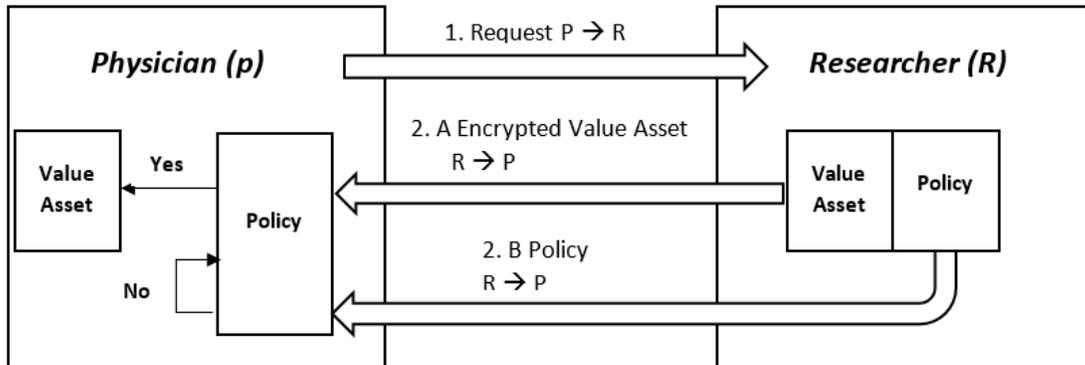


Figure 1. Privacy-Preserving Architecture

Research Question: What happens when the above scenario is scaled to include more than one physician and one researcher? What could be potential problems and solutions?

Conclusion

Based on the research on transitive workflows focusing on unanticipated revelation within the healthcare setting, we suggest following questions that need addressing in future:

1. What are the objectives in assessing privacy risk in a transitive health information workflow?
2. How can the privacy risk in cross-boundary organizations be quantified?
3. Where is the optimal balance in shared regulation between the organizational and governmental regulatory models?
4. What are key elements to be considered in a threat model policy?

References

Abraham, C., Watson, R. T., & Boudreau, M. C. (2008). Ubiquitous access: on the front lines of patient care and safety. *Communications of the ACM*, 51(6), 95-99.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society* (20:5), pp 313-324.

Big Data Report. 2014. *Big Data: Seizing Opportunities, Preserving Values*. Retrieved from http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1), 3-32.

Fung, B., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, 42(4), 14.

Fiebelkorn, A., Mehra, J., Salva, K., & Shetty, P. (2014). White paper for Information Assurance class, SUNY Buffalo.

Hersh, W. (2004). Health care information technology: progress and barriers. *Jama*, 292(18), 2273-2274.

HIPAA. (2004). Security White Papers. Workshop for Electronic Data Interchange.

ISO/DIS 31000 (2009). Risk management – Principles and guidelines on implementation. International Organization for Standardization.

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In *UbiComp 2001: Ubiquitous Computing* (pp. 273-291). Springer Berlin Heidelberg.

Lechler T., Wetzel S., Jankowski R. (2011). Identifying and Evaluating the Threat of Transitive Information Leakage in Healthcare Systems. In the Proceedings of the 44th HICSS, 1-10

NIST. 2014. “NIST Privacy Engineering Objectives and Risk Model Discussion Draft”. Retr Sept 2014

PIA. 2014. Guide to Undertaking Privacy Impact Assessments. Retrieved from <http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-undertaking-privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>

- PCAST. (2014). Report to the president on big data and privacy. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
- Sokolova, M., El Emam, K., Rose, S., Chowdhury, S., Neri, E., Jonker, E., Peyton, L. (2009). Personal health information leak prevention in heterogeneous texts. Biomedical Information Extraction International Workshop with the 7th International Conference on Recent Advances in Natural Language Processing
- Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Available at SSRN: <http://ssrn.com/abstract=667622>
- Tanna, G. B., Gupta, M., Rao, H. R., & Upadhyaya, S. (2005). Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. *Decision Support Systems*, 41(1), 242-261.
- Valecha, R., Upadhyaya, S., Rao, R., & Keepanasseril, A. (2012). An Activity Theory Approach to Leak Detection and Mitigation in Personal Health Information (PHI). Proc of WISP'12. Orlando, FL.
- Valecha, R., Kashyap, M., Rajeev, S., Rao, H.R., & Upadhyaya, S. (2014). An Activity Theory Approach to Specification of Access Control Policies in Transitive Health Workflows. Proc ICIS'14. NZ.
- Volonino, L., & Robinson, S. R. (2003). Principles and practice of information security. Prentice.
- Xiao, X., & Tao, Y. (2006). Anatomy: Simple and effective privacy preservation. In Proceedings of the 32nd international conference on Very large data bases (pp. 139-150). VLDB Endowment.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.
- Zwick, D., & Dholakia, N. (1999). Models of privacy in the digital age: Implications for marketing and e-commerce. Research Institute for Telecommunications and Information Marketing, University of Rhode Island.