What Sensitive Data-Sharing Examples Tell Us About the Potential for a National Health Monitoring System in America

A Research Paper
in STS 4600
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Systems Engineering

By

Hannah Katinas

April 10, 2020

Approved by Prof. Kent Wayland, Department of Engineering & Society

Introduction

It's hard to imagine a life without technology and the information that various technological devices are able to provide to us. In recent years, technology has become so intertwined in people's lives, that millions of Americans have become dependent on such information, such as fitness analytics or sleep trackers (Sapacz, Rockman, and Clark, 2016). Coupled with a continuously advancing healthcare field, it is possible for healthcare organizations to take advantage of these devices to collect data and monitor patient activity. Several propositions have been made for a national healthcare monitoring system, that would essentially track and monitor various types of data in order to understand overall health and potential interactions with various illnesses even better. Benefits of such a system include, but are not limited to, being able to alert users when they are displaying physical symptoms of illnesses, have come into contact with ill individuals, or require a doctor/hospital visit, and also the knowledge gained from all the data collected and the various health studies that will be made possible.

With increasing data privacy regulations that restrict that amount of information organizations are able to get from individuals, it is understandable why a healthcare system similar to this has not been put into place. Many data sharing applications are prone to breaches, so users may be highly skeptical of how secure this health monitoring system could really be. And with the nature of the system being highly sensitive and very personal, a data breach would potentially affect the lives of millions of citizens. If a national healthcare organization were to implement a monitoring system, data security would be a primary concern for not only the user's protection, but also for the organizations reputation, since a breach in health-related data in some cases may be equivalent in danger, if not more dangerous, than a breach in financial data.

In my research, I plan to examine data on similar systems to the potential national health monitoring one, and analyze what privacy conditions may need to be in place in order for it to be successful nationwide. I will be using two models to evaluate these similar systems that focus on how well that system addresses privacy concerns with its users and how well the system is designed and implemented. By looking into aspects of these systems such as reasons to why they failed/succeeded, benefits to its users, the scale of the system, any impeding regulations, and more, I hope to be able to conclude what elements need to be in place in order for a national health care monitoring system to be not only feasible, but also successful.

Background

In America, several healthcare systems are beginning to have the technology necessary to advance national health care by having some of the required components regarding big data, privacy, and security, that are required for early diagnosis and early prevention. (Kupwade and Seshadri, 20). The potential benefits of a national system that monitors its citizens' health data include faster illness detection, a decrease in dangerous mental health effects, lower health insurance rates, and decreased medical costs (Elbogen and Johnson, 2009). For example, if an individual had a device or application that were able to detect increased body temperature, cough detection, and etc., organizations would have more reliable data when conducting health studies or finding cures for various infections. Having this more reliable data would allow citizens to have more knowledge about illnesses and would enable them to self-diagnose themselves better. Additionally, with this increase of information, insurance companies would have less risk when insuring their clients, which in turn would lower their clients' overall health insurance costs. One of the reasons that a system like this is not an immediate goal for the near future is that there are

so many privacy concerns regarding American citizens handing over their sensitive information to any government or corporation.

Technological Obstacles

One of the many obstacles preventing a national healthcare monitoring/survaeillance system from being implemented in America is that the specific technology and the systems needed to support the technology and the data do not yet exist, or have not yet been tested. There are several remote patient monitoring devices available for health care workers to track a patient's vitals or other levels at any time. Most of these are designed for specific illnesses, such as a blood glucose level reading for diabetes, or portable ECG (electrocardiogram) readers for patients with heart arrhythmias (Kugler, Lohmüller, Eskofier, 2012). With the recent boom in cellphone applications, there are many applications designed for similar uses that people can now download directly such as blood pressure monitors or instant heart rate readers. There are also technological devices that these applications can connect to in order to monitor such data. However, there is not an application that currently exists that tracks and monitors multiple different elements of a person's health, uses that data to then make conclusions about their health, and then reports these conclusions to a larger organization.

The technical project that my team is working on focuses on an application that could potentially do what has been described above. It collects data from various smartphone sensors in order to understand the user's daily activities so that when some aspects of the data are different from the baseline readings, the app can start to predict some possible meanings for this difference. For example, if a healthy user comes into contact with a user who has been labeled as "ill" (based on sensors such as heart rate, acceleration, or sleep detection) and then starts displaying some of the same data as this ill user, the app can indicate that they may both now ill.

The ultimate goal of the research is to create "a mobile application that passively assesses a (person's) readiness immediately and over time," (Patel, n.d., para. 5). By building predictive health analytics that utilize smartphone sensors, the monitoring and tracking of various illnesses among certain populations can be noticed and understood in real-time.

Regulatory Obstacles

Another major obstacle in the way of a national health monitoring system is legislation surrounding data privacy. Since the way in which data breaches occur are always evolving in order to stay ahead of data protection measures, United States data privacy regulations are also always evolving to try to keep user's data secure. Because of this, there are hundreds of very specific federal legislations that a company has to follow when attempting to extract data from their users. There are also state regulations put in place that differ from state to state.

There are two general types of regulations that exist when it comes to mHealth (mobile health) applications. The first type of regulations are designed to prevent erroneous diagnosis if the application were to be misused or were to malfunction, which could potentially case a huge risk to the general public (Kemal Yetisen, Martinez-Hurtado, Vasconcello, Simsekler, Akram, Lowe (2014)). These regulations and guidelines are set by the FDA (Food and Drug Administration), and mobile applications that essentially seek to replace a doctor's visit are being kept under a close eye by the FDA because there exists such a risk for a user's wellbeing.

The second type of regulations are those enforced by certain federal and state agencies issued with protecting the privacy of individual's data, especially their health information (Munos, Baker, Bot, Crouthamel, Vries, Ferguson, Hixson, Malek, Mastrototaro, Misra, Ozcan, Sacks, Wang, (2016)). For example, any biosensors or apps that collect or transmit information using radio technology, such as Bluetooth, are subject to regulation by the FCC (Federal

Communications Commission) to ensure safety of the product and no interference to other radio services. If there is health information being collected, it must abide by HIPAA (Health Insurance Portability and Accountability Act) as well as the general data privacy rules that apply to all other applications, which are mostly enforced by the Federal Trade Commission.

Identifying Models Used to Evaluate Sensitive Data Sharing Systems

There is research that has been done that explains some background on the topic of health monitoring systems, the effects they have had on communities, and how to potentially evaluate these them. In order to effectively assess some examples of systems similar to the national health monitoring system, there needed to be a way of identifying key elements that could also be applied to different types of systems. Described below are two models that can be used to determine how successful a system is when it comes to dealing with privacy conditions.

Firstly, Zhou Xu (2019) discusses the introduction of online databases storing patient health information and how it has influenced patient's privacy concerns. With his background in information technology and public administration, Xu effectively explains that health informatics, which is when technology is used to organize and analyze health records to improve health outcomes, has helped reduce healthcare costs and improve healthcare efficiency in hospitals and other large treatment centers. However, having patients' personal health information on these systems exposes privacy risks and has made patients much more sensitive for their personal health information. With continuous threats of data breaches or hackers, the users involved in this system must be able to trust their health organization enough to want to participate.

Xu performed a study in which they were able to provide a framework for a better understanding of the formation and the consequences of these information privacy concerns. The results of this study indicated that there were five factors that determined a patient's privacy concerns. These five factors were: privacy awareness, perceived informativeness, information sensitivity, regulatory expectations, and importance of information transparency (Figure 1).

Figure 1. Model #1: Determining How Well a System Addresses Privacy Concerns

Factor	Description
(1) Privacy Awareness (individual level)	The more a patient is aware of the privacy issues, the more they will be concerned. In simplistic terms, ignorance is bliss. If a patient is not aware of a privacy issue, that means they cannot become concerned with that privacy issue.
(2) Perceived Informativeness (service level)	If the patient is given access to more of their health information, they will have more privacy concerns.
(3) Information Sensitivity (information level)	Personal health information is the most sensitive type of information, and will increase a patient's privacy concerns.
(4) Regulatory Expectations (macro-environment level)	The patient will have fewer privacy concerns if he/she believes that the organization or government conducts more regulations on service providers.
(5) Importance of Information Transparency (organization level)	The more a patient is aware of their personal health information privacy, the more they will be concerned.

In my research, these five factors are a way for the examples of sensitive data-sharing systems to be examined and analyzed. With a model such as this one, business managers and government organizations are provided with a practical framework to conduct appropriate studies in order to reduce the privacy concerns of patients while also focusing on protecting their sensitive information. If there is a previous system that has not succeeded due to a lack of patient trust, it may be because one or more of these five factors was not made a priority.

Another piece of research that will be reviewed discusses why users may be hesitant to participate in a telehealth (telecommunication technologies for health information) system, and ways in which these telehealth organizations can increase trust between their users and

themselves (Zaidan, Zaidan, and Kiah, 2011). The authors of this article, whom are all professors in Data Communication and Computer Science, state that the issue of trust in any online service involves privacy, which is defined as protecting personal information, and security, which refers to protecting the website from attack and/or misuse. When privacy and security are breached on health websites, it can affect users' trust and confidence towards that e-health service, and even hinder them from using other e-health services.

Zaiden et al. found that the successful implementation of telemedicine is related to the availability of three factors: strong fundamental knowledge and infrastructure, planning and management of health information and technology, and fulfillment of legal and ethical issues and constant evaluation of telemedicine implementation (Figure 2). These three factors are another way to evaluate the other sensitive data-sharing systems that will be analyzed later.

Figure 2. Model #1: Assessing the Design and Implementation of a System

Factor	Description
(1) Strong Fundamental Knowledge and Infrastructure	An organizational structure that efficiently and directly assesses information to meet the end goal.
(2) Planning and Management of Health Information and Technology	A system in which health information is managed securely and accurately.
(3) Fulfillment of Legal and Ethical Issues and Constant Evaluation of Telemedicine	Making sure that the technology used is operating within up-to-date regulations and are not causing any ethical issues.

Methods

When looking for other sensitive data-sharing examples that were used as a comparison to the national health monitoring system discussed earlier, there were two main elements that the search was focused around. The first element of the system that I searched for is a case in which there were similar privacy concerns to those that exist in telehealth systems. This can be relating to privacy, security, or authentication. The other element that I focused on when finding evidence of other examples of sensitive data-sharing systems was the idea of people willingly

giving their sensitive data over to an organization. This indicates that the system has a level of trust with their user's and they are able to make them feel secure enough in their system to provide their health data, which is an important part of ensuring the success of a system like this. In order to ensure that the evidence being found was authentic and reliable, I concentrated the search on published journal articles that have data and statistical findings to support their conclusions.

Once a few existing systems with the elements described above were identified, a case analysis was done on the examples at hand. The two models described above were used to evaluate the existing system. Model #1 was used to evaluate how well the system ensured trust and confidentiality with their participants, and Model #2 was used to determine how well the system was designed and implemented.

Once the models were applied to the data-sharing examples that were found, similarities between the national health monitoring system and the analyzed example were identified to ensure that both systems have similar aspects to them and are connected in some ways. Then, differences were explained, as well as reasons as to why these differences exist, what these differences have resulted in, and ultimately, if these different features are feasible in the potential national health monitoring system in order for it to be a success.

Findings

German Public Health Records

One of the studies that I will be analyzing involves Personal Health Records (PHR) in Germany (Ploner, Neurath, Schoenthaler, Zielke, and Prokosch, 2019). There are multiple PHR systems in the country that currently exist, but Germany has yet to widely adopt a single infrastructure. With a public cloud computing system and smart phone application already in the

works, the researchers of this study wanted to understand the trust and privacy aspect of such a widely used system. The results of their study were that people typically trust healthcare providers more than private companies, and that a system like this, paired with the right data security, can be successfully implemented in Germany.

If the German PHR system can be framed by Model #1 and is expected to be successful, that means Model #1 may be able to be mapped to a health monitoring system in America. Since the majority of the users in the PHR system trusted their health care providers with their health information (most likely due to their trust in the doctor-patient confidentiality agreement), they were not completely aware of the privacy issues or their personal health information privacy, because they did not feel a need to look into it. According to this model, this is exactly what is needed in the privacy awareness category and the importance of information transparency category for a system to minimize privacy concerns with its users. In other words, the patients trusted their doctor, which made them not feel encouraged to research the privacy risks associated with the PHR system. Because of this, they had limited knowledge about the risks and limited concerns about them as well. In terms of regulatory expectations, the patients understand that there are many regulations that healthcare providers must follow, which also helps minimize the privacy concerns in this category. The perceived informativeness and information sensitivity levels of this PHR system indicate that there will be a lot of privacy concerns among the patients, but this is expected when dealing with personal health information like this.

Figure 3. Model #1: Determining How Well a System Addresses Privacy Concerns	
Factor	**German PHR System**
(1) Privacy Awareness (individual level)	Participants are not that aware of the privacy issues regarding health-related data, so they have no knowledge of any risks to be concerned about.
(2) Perceived Informativeness (service level)	Participants were given access to their health information, so they had privacy concerns.
(3) Information Sensitivity (information level)	Since this system involved personal health information, this increased the participant's privacy concerns.
(4) Regulatory Expectations (macro-environment level)	Participants understood that their healthcare provider had regulations that must be followed, so they were less concerned.
(5) Importance of Information Transparency (organization level)	Participants are not that aware of the personal health information privacy issues, so they are not that concerned either.

The creators of the German PHR system seem to have understood the importance of each of Model #2's factors when it comes to the system's implementation. All the patient data was stored through public cloud computing. For the factor of "Planning and Management of Health Information and Technology", this storage method, along with additional security measures, ensured that all health information was de-identified and secure. When patients had to interact with the application, they never had to input personal information, and all of their data was linked to a unique identifier instead of the patient's name. Basic cloud computing also ensures that certain laws and regulations under the German Data Protection Act are put into place to help protect the data, which falls into the category "Fulfillment of Legal and Ethical Issues and Constant Evaluation of Telemedicine". Lastly, the entire structure of the system was well thought out, with the security and the confidence of the patients being one of the top priorities, which makes the system deemed a success under the factor "Strong Fundamental Knowledge and Infrastructure".

Figure 4. Model #2: Assessing the Design and Implementation of a System	
Factor	**German PHR System**
(1) Strong Fundamental Knowledge and Infrastructure	The security and the confidence of the participants were the system's top priority.
(2) Planning and Management of Health Information and Technology	All health information was stored on public cloud computing, which ensured that all information was de-identified and secure.
(3) Fulfillment of Legal and Ethical Issues and Constant Evaluation of Telemedicine	Data was protected under the German Data Protection Act.

Mental Health Mobile Application in the Dominican Republic

The other research study that I will analyze is a study done with a mental health mobile application in the Dominican Republic (Caplin, Lovera, and Liberato, 2018). It focuses on acceptance, appropriateness, engagement, and work processes of the entire system. The results of the study concluded that there was a pretty low retention rate and low patient engagement. Using the models, we can try to understand what factors this system did not accomplish so that we can better understand what factors are necessary in the implementation of a national health monitoring system.

Since Model #1 focuses more on the privacy issues and how transparent they are to the participants, it was a little difficult to analyze this Dominican Republic system since the researchers did not focus on their privacy issues or transparency with the clients. However, there were several factors that were easy to assess. For information sensitivity, since the system is dealing with personal health data, there was an increased amount of concern among participants. With regulatory expectations and privacy awareness, the participants were made aware of the HIPPA and FDA regulations that were put in place to protect them from various privacy issues, which helped lower their privacy concerns.

Figure 5. Model #1: Determining How Well a System Addresses Privacy Concerns	
Factor	**Dominican Republic Mental Health System**
(1) Privacy Awareness (individual level)	The participants were aware of the privacy issues but this was combated with their awareness of the regulations.
(2) Perceived Informativeness (service level)	Not discussed in the study.
(3) Information Sensitivity (information level)	Since this system involved personal health information, this increased the participant's privacy concerns.
(4) Regulatory Expectations (macro-environment level)	There were HIPPA and FDA regulations (this was a collaboration between Rutgers University and University Autónoma de Santo Domingo), so the participants had fewer privacy concerns.
(5) Importance of Information Transparency (organization level)	Not discussed in the study.

Under Model #2, the mental health application in the Dominican Republic did not perform as well as the German PHR system. The difference between the two systems can be seen in the "Strong Fundamental Knowledge and Infrastructure" factor. In this system, it was reported that there was a low retention rate due to several potential reasons (ethnic diversity, language diversity, the complexity of the tasks that the application provides, etc.). This system did however successfully have the other two factors, which were "Planning and Management of Health Information and Technology" and "Fulfillment of Legal and Ethical Issues and Constant Evaluation of Telemedicine". This was done by using anonymous pseudonyms that were linked to participant numbers, and by following FDA and HIPPA guidelines.

Figure 6. Model 2: Assessing the Design and Implementation of a System	
Factor	**Dominican Republic Mental Health System**
(1) Strong Fundamental Knowledge and Infrastructure	There were several hypothesized reasons as to why this system was not strong.
(2) Planning and Management of Health Information and Technology	Anonymous pseudonyms were used instead of personal information.
(3) Fulfillment of Legal and Ethical Issues and Constant Evaluation of Telemedicine	De-identifying the patient's information helped keep the study within regulations.

Significance

There are quite a few key points and findings that can be taken from both the German PHR system and the Dominican Republic mental health system, and mapped onto the potential national health monitoring system. The German PHR system study showed that having this national system provided by a private company is not ideal. Having a government organization be the main provider would increase trust since there would have to be a lot of regulations in place. Additionally, people tend to think that the driving force behind private companies is making a profit, whereas for government organizations there may be more trust. This of course varies from country to country, and even varies within America. However, the German PHR study showed that overall, a government organization would increase trust within the participants.

These two case studies also indicate some ways that may keep retention rates of the users high. Similar to the Dominican Republic mental health system, basing the national monitoring system on hospital visits may be a good starting point. If they agree to do so, users will be able to simply download a mobile application that the doctor suggests and will be more likely to trust the application because their health is more at stake than someone who hasn't visited the hospital recently. Another way of keeping the retention rates high would be to make the national health monitoring application extremely passive (not requiring a lot of user interaction). When first downloading the application, participants may need to sign a waiver allowing access to a partial medical record as a baseline, which would allow passive monitoring of activity to lead to more accurate results.

One of the key takeaways from both systems is that the less aware the users are about privacy issues, the more they are willing to trust the system. For example, a user that is not

familiar with data breaches and the risks associated with sensitive data will have more trust in a system that deals with this data than a user who is familiar with these risks. With government organizations, this is hard to do because a lot of that information is made public. But a way to combat this is to instead focus on all the regulations put in place to prevent these privacy issues from arising. If this information is presented to users in a way that makes them feel protected rather than at risk, they will gain more trust in the system.

Conclusion

By combining the continuous technological advancements in the healthcare field with data analytics, a national health monitoring system is a major possibility. It would be a way to track and monitor various types of data so that a better understanding of the overall health of participants could be achieved. After analyzing a PHR system in Germany and a mental health system in the Dominican Republic, there are several key takeaways that would help in the design and implementation of a successful national health monitoring system. These takeaways include ways to increase user trust in the goals of such a system, ways to increase user retention rates, and ways to make participants feel protected from data breaches rather than at risk to them. With a successful national system in place, benefits such as lower healthcare costs, faster illness detection, and the possibility of conducting more health studies may be achieved.

References

2019 Capital One Cyber Incident | What Happened | Capital One. (n.d.). Retrieved February 21, 2020, from https://www.capitalone.com/facts2019/

Caplan, S., Sosa Lovera, A., & Reyna Liberato, P. (2018). A feasibility study of a mental health mobile app in the Dominican Republic: The untold story. *International Journal of Mental Health*, *47*(4), 311–345. https://doi.org/10.1080/00207411.2018.1553486

Chunhua, W., Tianyong, H., Carol, F., & John, H. (2019). Crowdsourcing Public Opinion for Sharing Medical Records for the Advancement of Science. *Studies in Health Technology and Informatics*, 1393–1397. https://doi.org/10.3233/SHTI190456

Elbogen, E. B., & Johnson, S. C. (2009). The Intricate Link Between Violence and Mental Disorder: Results From the National Epidemiologic Survey on Alcohol and Related Conditions. *Archives of General Psychiatry*, *66*(2), 152. https://doi.org/10.1001/archgenpsychiatry.2008.537

Gradl, S., Kugler, P., Lohmüller, C., & Eskofier, B. (2012). Real-time ECG monitoring and arrhythmia detection using Android-based mobile devices. *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2452–2455. https://doi.org/10.1109/EMBC.2012.6346460

Kemal Yetisen, A., L. Martinez-Hurtado, J., Vasconcellos, F. da C., Emre Simsekler, M. C., Safwan Akram, M., & R. Lowe, C. (2014). The regulation of mobile medical applications. *Lab on a Chip*, *14*(5), 833–840. https://doi.org/10.1039/C3LC51235E

Kupwade Patil, H., & Seshadri, R. (2014). Big Data Security and Privacy Issues in Healthcare. *2014 IEEE International Congress on Big Data*, 762–765. https://doi.org/10.1109/BigData.Congress.2014.112

Munos, B., Baker, P. C., Bot, B. M., Crouthamel, M., Vries, G. de, Ferguson, I., Hixson, J. D., Malek, L. A., Mastrototaro, J. J., Misra, V., Ozcan, A., Sacks, L., & Wang, P. (2016). Mobile health: The power of wearables, sensors, and apps to transform clinical trials. *Annals of the New York Academy of Sciences*, *1375*(1), 3–18. https://doi.org/10.1111/nyas.13117

Patel, T. (n.d.). Warfighter analytics using smartphones for health. Arlington, VA: DARPA: Defense Advanced Research Projects Agency website: https://www.darpa.mil/program/warfighter-analytics-using-smartphones-for-health

Ploner, N., Neurath, M. F., Schoenthaler, M., Zielke, A., & Prokosch, H.-U. (2019). Concept to gain trust for a German personal health record system using public cloud and FHIR. *Journal of Biomedical Informatics*, *95*, 103212. https://doi.org/10.1016/j.jbi.2019.103212

Sapacz, M., Rockman, G., & Clark, J. (2016). Are we addicted to our cell phones? *Computers in Human Behavior*, *57*, 153–159. https://doi.org/10.1016/j.chb.2015.12.004

Xu, Z. (2019). An empirical study of patients' privacy concerns for health informatics as a service. *Technological Forecasting & Social Change*, *143*, 297–306. https://doi.org/10.1016/j.techfore.2019.01.018

Zaidan, B., Zaidan, A., & Kiah, M. M. (2001). Impact of Data Privacy and Confidentiality on Developing Telemedicine Applications: A Review Participants Opinion and Expert Concerns. *International Journal of Pharmacology,* 7(3), 382-387. doi: 10.3923/ijp.2011.382.387