Proceedings of the International Conference on Industrial Engineering and Operations Management
Pilsen, Czech Republic, July 23-26, 2019

Process View on E-Health with Risk Analysis

Michal Švehla and Jiří Tupa
Department of Technologies and Measurement
Regional Innovation Centre for Electrical Engineering (RICE)
Faculty of Electrical Engineering
University of West Bohemia
Univerzitní 2732/8, 301 00 Plzeň 3
svehlam@rice.zcu.cz, tupa@ket.zcu.cz

Abstract

While technology is evolving to be more patient oriented to provide a better care for them. How the e-Health works from process view is a bit uncertainty about how. Many security questions need to be solved before using an e-Health as a tool for a wide range of people. There is also a one about e-Health itself. Field of e-Health is gaining more and more attention considering we are going through industry revolution 4.0. Research provides process perspective on this issue including a risk analysis together with structured process map from patient/user to his social worker for example doctor, nurse or other medical personnel. This model should serve as a basic template for better understanding and easier implementing an e-Health almost anywhere.

Keywords: e-Health, Process, Modeling, Risk Analysis, Industry 4.0

1. Introduction

Fourth industrial revolution is a keyword in many current research papers. This term has impact on different areas of our life. One example is healthcare services. The current literature discusses this issue under a term e-Health. The e-Health is being mode and more popular to provide quality and less expensive healthcare service [1]–[4]. The implementation of the e-health concept represents not only the implementation of an appropriate information infrastructure, but also a description of the processes that will be implemented within the framework of digitized agendas. Therefore, an example of development a process model will be the subject of this article

On the other hand, many applications for e-Health Internet connection and accessing medical data through a secure platform immediately. Medical data of users, doctors and healthcare companies are a big target of focus concerning their security and privacy. This creates a wide area of research, where mostly a security and privacy issues are solved.

Currently, the issue is not solved by many e-health related processes in present research. Focus of this work is to propose a process model of e-Health communication, how it works, what risks it involves and how it contributes to quality management system. So when you want to improve something you have to start at a model. This process model is completely explained later in paper. Second part is a brief example of e-health security problematic parts. It is not possible to cover every aspect, framework, communication or certain part of e-Health by this work. Mentions about those aspects are for pointing out their existence.

Last part is a risk analysis based on process model. Tables in this work shows vulnerability and their score from a subjective point of view. The next table follows the vulnerability table and shows a qualitative risk analysis. From this table a complete risk analysis created together with risk management plan which is explained.

Main issue solved in this paper is to show a more detailed model of communication between patient, doctor and healthcare company. Based on this model and data which were obtained by interviews there is a risk analysis which focuses on threats and vulnerabilities and measures to them.

2. Literature review

Many articles mentioned issue about e-Health in relation with information security and data protection [1], [3], [4]. Although all of them are focused on same topic, everyone is giving a new perspective. In first article is a security framework for authentication and data transmission. Framework consists of protocol architecture, which

provides data security, channel security, encryption algorithms for data transmission and when there is a need for different variations of e-Health in different scenarios there are two risk adaptive authentication techniques. Just several approaches related to this topic were found, for example [5], [6], [7], [8]. [1]

Second article is focused on privacy, security and trust services in e-Health specifically about mobile component and it provides an innovative infrastructure framework. New challenges rises thanks to new (mobile) sources of e-Health. For those challenges a number of solutions that deal with secure data transfer have been studied [9], [10]. After studying related work to theirs, main focus is on e-Health mobile PST requirements and data sources and types. For example, requirements can be expressed in general as security, privacy and trust. As a data sources and types can be represented by messaging standards, patient and clinical support system, research portal and organization connected to e-Health problematic. Another part is focused on e-Health security services their mechanism. [3]

Articles above should serve as a brief example of how complex a security in e-Health is and what are the obstacles in this field.

3. Process model

Based on the study of literature, a process model was proposed which describes the basic relationships between the stakeholders in the e-health concept. The model presents Figure 1.

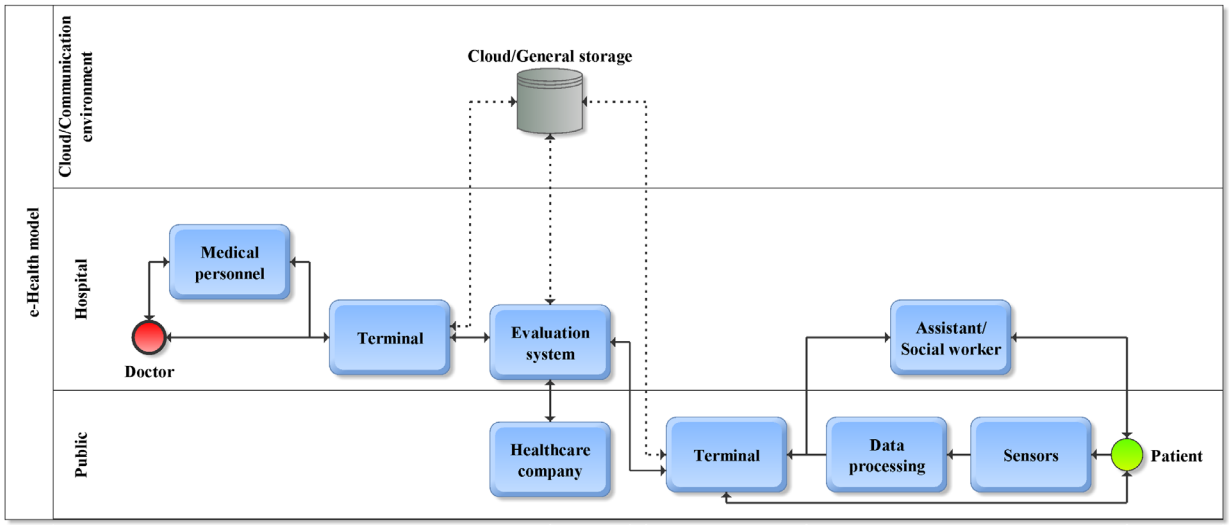

Fig. 1. E-Health communication process map

This part of the paper will be an explanation of process model. This perspective has a starting point in patient where sensors measure patient's essential body functions for example pulse rate, temperature, respiration rate. All of those data need to be processed and that occurs in data processing, which is next on this communication line. Assuming that sensors and data processing works fine, patient can operate terminal on his own. On the other hand, some patients are not able to move or function on their own, so they must have an assistant or social worker.

Terminal is representing access point for patients data through a PC, tablet, mobile phone maybe even through a television. There are so many options in the future.

Next section of this model is a cloud storage, evaluation system and a healthcare company. Cloud storage contain all the data transferred between patient, doctor, evaluation system and healthcare company. Data goes from the terminal to cloud/general storage and evaluation system. There is an idea of double-checking transferred data and having a small backup when cloud is not working. Therefore, when cloud is out a relatively small local memory could substitute main storage (cloud/general storage) in case of emergency.

Data sources can really test a network capacity by generating thousands gigabytes of data transmission in network. There are solutions for it, for example in [2] there are few predominant examples of Big Data technologies of computation systems (MapReduce, Hadoop, STORM). They cannot be used directly to fulfill its purpose. There have to be some additional capabilities to them. So the use of Big Data and its capabilities can be also found in [2].

For example how this part between terminals should work. Terminal on the patient side is transmitting data to cloud storage and to evaluation system. In theory, this part should be something like a brain of this system. On its own, it should decide and contact doctor or medical personnel through another terminal. In addition, it could automatically send a message to healthcare company based on doctor opinion and prescription. Healthcare company then could manufacture and send a medicine to a pharmacy and at the same time system should contact a patient or his assistant or social worker when his medicine will be available at the closest pharmacy.

All of this should be a process model of communication between patient, doctor and healthcare company for communication and authentication for e-Health.

For comparison there are similar models which shows a concept of e-Health system. First one (Fig 2) shows a general e-Health environment. Cloud is the center for whole communication in this concept. Communication with other parts (doctor, medical staff, hospital, etc.) occurs through standard (healthcare records). At center of the cloud is a DHC which stands for digital healthcare.

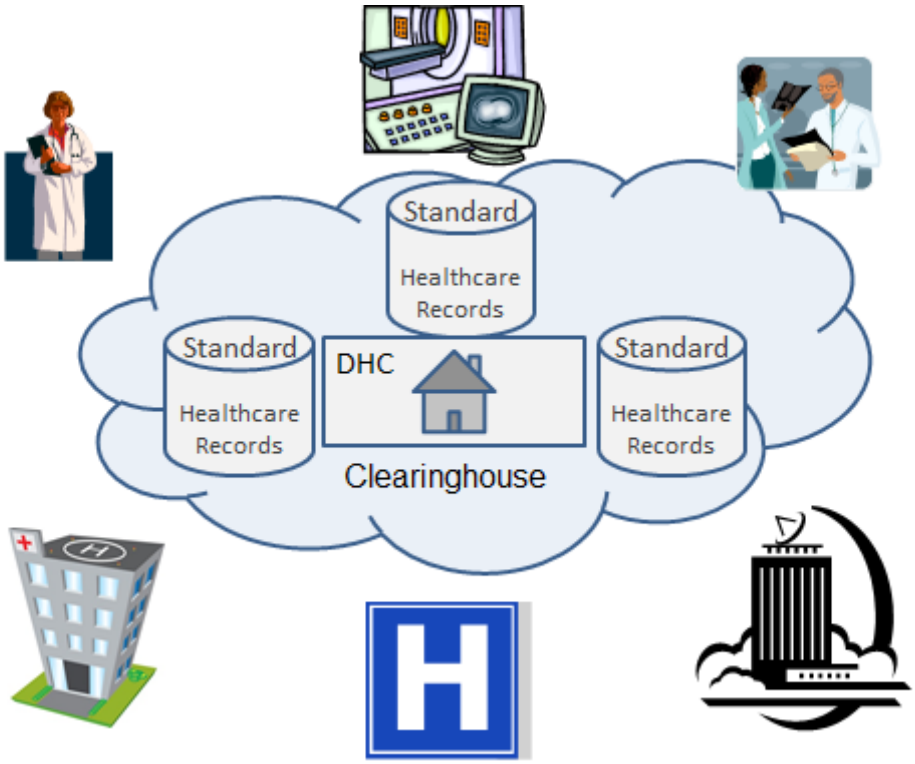

Fig. 2. General e-Health environment [3]

Another model, which can contribute to detailed model in Fig. 1, is shown in Fig. 3. It shows a basic communication through Wi-Fi between patient and his body sensors and doctor which can access database.

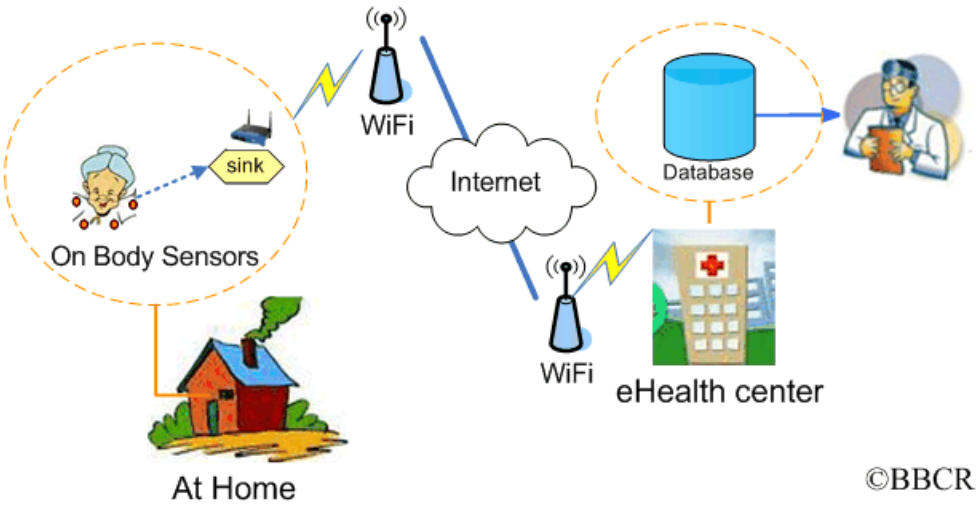

Fig. 3. Communication in e-Health [11]

4. Risk analysis

The previous part of this paper was focused on security aspects of e-Health issue. Risk analysis is based on previously proposed model in figure 1 and model itself is based on literature review and other similar models. Every part of the model can generate various vulnerabilities. That is shown in table 1. The fourth industrial revolution is bringing us many benefits but also many threats as the goal is to get everything digitized. It follows that our private data needs to be properly protected against hacker or anybody who is not authorized to see it.

The first step there should be an asset and threat analysis which take part in e-Health service. In this case assets are electronic records, cloud/general storage, software, computers, hospital staff, healthcare company employees and healthcare company (as a supplier). Threats that are present are following: fire, network outage, failure of the cooling device, data leakage, equipment failure, employee failure, infecting the terminal/network, poorly programmed evaluation system and loss of access codes. All assets and threats together are making a table of vulnerabilities which are assessed.

The assets and threats are rated from 1 to 5 meaning that number 1 is least probable or with the least significant value and with number 5 is just in opposite.

Table 1. List of vulnerabilities

Vulnerabilities	Asset description	Electronic records	Cloud/Local data storage	Software	Computers	Hospital staff	Healthcare company employees	Healthcare company (as a supplier)
	Asset value	**4**	**4**	**3**	**3**	**3**	**4**	**4**
Description of the threat	**Likelihood of threat**							
Fire	**1**		1		2			
Network outage	**2**	1	1		1			
Failure of the cooling device	**3**	1	5		3			
Data leakage	**3**	5	5	2	5	5	5	4
Equipment failure	**3**	5	4	4	3			5
Employee failure	**4**	5		4	2	2		3
Infecting the terminal/network	**5**	5	4	4	5		4	
Poorly programmed evaluation systém	**2**					2	3	3
Loss of access codes	**3**	2	2		2	2	2	

Table 2. Qualitative risk analysis

Vulnerabilities	Asset description	Electronic records	Cloud/Local data storage	Software	Computers	Hospital staff	Healthcare company employees	Healthcare company (as a supplier)
	Asset value	4	4	3	3	3	4	4
Description of the threat	Likelihood of threat							
Fire	1		4		6			
Network outage	2	8	8		6			
Failure of the cooling device	3	12	60		27			
Data leakage	3	60	60	18	45	45	60	48
Equipment failure	3	60	48	36	27			60
Employee failure	4	80		48	24	24		48
Infecting the terminal/network	5	100	80	60	75		80	
Poorly programmed evaluation system	2					12	24	24
Loss of access codes	3	24	24		18	18		
Acceptable	0-29		To watch	30-58			Unacceptable	59-100

Table 3. Risk management plan

Asset	Threat	Name of risk	Precaution	Responsible person
Electronic records	Data leakage	Leakage of sensitive information	Extra firewall with antivirus, access with permission	Employees
Electronic records	Equipment failure	Unavailability of information	Backup power supplies	Hospital management
Electronic records	Employee failure	Leakage of sensitive information	Software control	IT company (External)
Electronic records	Infecting the terminal/network	Loss or leakage of information	Extra firewall with antivirus	IT company (External)
Cloud/Local data storage	Failure of the cooling device	Unavailability of information	System monitoring of the cooling system	External company
Cloud/Local data storage	Data leakage	Loss of common and archived files	Data backup to external company servers, access with permission	External company
Cloud/Local data storage	Infecting the terminal/network	Inaccessibility or loss of information	Backup data to external HDD	Owner of cloud/general data storage
Software	Infecting the terminal/network	Loss of information, local network corruption, unauthorized access	Prohibition of installing third-party software without permission, training	Employees
Computers	Infecting the terminal/network	Loss or leakage of information	Checkpoints of external devices, prohibiting the use of their own external devices without control	Employees
Healthcare company employees	Infecting the terminal/network	Loss or leakage of information	Antivirus and spyware control of emails, employee training, external device control	Employees
Healthcare company (as a supplier)	Equipment failure	Failure to deliver the contract within the deadline	External repair firm with 24/7 service	Owner of healthcare company

In this section will be about detailed description of risk analysis in tables above. The most important is the final table where the assets, threats and risks with precaution and also a responsible person.

First asset for evaluation is electronic records. They contain a personal data about assigned doctor, patients personal and their treatment data. Threats that are possible to happen to electronic records are data leakage, equipment and employee failure and infection of the terminal/network. Data leakage in electronic record is one of the most problematic one because it is a very complex one. It can happen by unintentionally or deliberately both doctors and patient by their terminal where medical personnel and assistant or social worker have access. Unintentionally means that data leaked through attack or virus that was downloaded or uploaded by accident. There should be a control in form of monitored access with permission for everyone that can access it and with extra firewall and antivirus. The next thing is if equipment is not working in terms of power failure and this results in the unavailability of medical data. In those critical points there should be a secondary power supply to power them up and keep communication chain active.

Another valuable asset is a data store, which can be both cloud storage and local. Both have the possibility of overheating because they need to be properly cooled. Overheating can lead to data unavailability, loss or inaccessibility of information. Exact threats, which can occur, can be failure of the cooling device. To prevent that from happening, there should be monitoring system that can warn supervisor that system server or hard disk is overheating. As a prevention to data leakage some form of backup to external company for all data. When infection occurs either of terminal or whole network there could be a case of virus that deletes data or somehow modifies them and eventually can erase them.

That leads to another threat which through virus can rise to the occasion infect and influence our data. This threat can come through the software. Prohibition of installing third party software without permission to the computer should prevent from this to happen. Training should be introduced as a complement to this measure.

Prevention to same threat but in terms of hardware is to implement checkpoints of external devices and together with that prohibit connecting external devices to computer.

Last and very important part is a healthcare company. Their access to data is quite extensive and chance of a threat is very high. Precaution for infecting a communication network or a terminal (terminal is a local PC in the company) is quite similar to threats with connection to infecting. An extended antivirus and spyware control of emails should be in place together with employee training whit what their actions could do. Equipment failure for healthcare company could mean failure to deliver order within a given deadline.

5. Conclusion

This paper tried to introduce the issue e-Health in context of process modeling and risk management. Major contribution of this work is a non-technical point of view on problematic in e-Health. Firstly, a process model of communication between patient, doctor and healthcare company for e-Health has been described. E-Health is gaining more and more attention to be a subject of study from security point of view. Quality management now can start continuous improvements to a proposed model. This sets a capability maturity model to a level 3 because this paper defined a process of communication in e-Health.

Secondly, this work contains a risk analysis of mentioned model. Risk analysis is based on model that is proposed and together with this, there are three tables that shows how certain risks were assessed. First table is for assessing asset value and threats that can occur. Second table shows a qualitative risk analysis and this table gives foundation to a risk management plan. Risk management plan consists of threats, risks and measures how to manage risks.

The possibilities of implementing process management and risk management as an essential element of the E-health concept will be the subject of further research.

Acknowledgements

This research has been supported by the Ministry of Education, Youth and Sports of the Czech Republic under the RICE – New Technologies and Concepts for Smart Industrial Systems, project No. LO1607, and by the Technology Agency of the Czech Republic under the project Software platform to accelerate the implementation of management systems and process automation — project No. TH02010577.

BIBLIOGRAPHY

[1] A. Boonyarattaphan, Y. Bai, and S. Chung, “A security framework for e-Health service authentication and e-Health data transmission,” *2009 9th Int. Symp. Commun. Inf. Technol. Isc. 2009*, pp. 1213–1218, 2009.

[2] W. Liu and E. K. Park, "Big data as an e-health service," *2014 Int. Conf. Comput. Netw. Commun. ICNC 2014*, pp. 982–988, 2014.
[3] W. Liu, E. K. Park, and S. S. Zhu, "E-Health PST (privacy, security and trust) mobile networking infrastructure," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, pp. 1–6, 2014.
[4] A. Michalas, N. Paladi, and C. Gehrmann, "Security aspects of e-Health systems migration to the cloud," *2014 IEEE 16th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2014*, pp. 212–218, 2014.
[5] K. Christopher, D. Curtis, and O. T. Ertem, "Security Architecture," p. 69, 2001.
[6] S. Han, G. Skinner, V. Potdar, and E. Chang, "A framework of authentication and authorization for e-health services," p. 105, 2007.
[7] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S. Khan, "Timestamp authentication protocol for remote monitoring in eHealth," *Proc. 2nd Int. Conf. Pervasive Comput. Technol. Healthc. 2008, PervasiveHealth*, pp. 73–76, 2008.
[8] G. Russello, C. Dong, and N. Dulay, "A workflow-based access control framework for e-Health applications," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 111–120, 2008.
[9] W. Liu and E. K. Park, "e-Healthcare security solution framework," *2012 21st Int. Conf. Comput. Commun. Networks, ICCCN 2012 - Proc.*, pp. 1–6, 2012.
[10] S. D. Cannoy and A. F. Salam, "A framework for health care information assurance policy and compliance," *Commun. ACM*, vol. 53, no. 3, p. 126, 2010.
[11] W*elcome to BBCR Group* [online].Copyright ©2009. Available from: https://bbcr.uwaterloo.ca/~x27liang/seehealthbib.htm

Biographies

Michal Švehla is a student of doctoral study program at faculty of Electrical Engineering University of West Bohemia in Pilsen. He is in first year of this program. Before doctoral study he earned Bachelor and Master degree in the same University as mentioned above. His research interests include e-Health/healthcare, processes, optimization.

Jiří Tupa received his MSc (2002) and PhD (2006) in Electrical Engineering from Faculty of Electrical Engineering, University of West Bohemia in Pilsen in Czech Republic. He is a Vice-dean of faculty and Senior Lecturer at Department of Technologies and Measurement. Dr. Tupa is member of executive management at Regional Innovation Centre for Electrical Engineering of the Faculty of Electrical Engineering at the University of West Bohemia in Pilsen. He is also PhD supervisor, reviewer of journal and conference publications and co-organizer of conferences.

His research interests include Business Process Management, Quality Management, Risk and Performance Management in Electrical Engineering Industry, Industrial Engineering, Electronics Manufacturing and Diagnostics, Financial and Project Management, Copyrights and patents law, information law and transfer of IPR. Jiri Tupa is responsible for several international research and development projects with industrial and University partners.