International Journal of Operations Management

ResearchLEAP

Volume 1, Issue 2, January 2021, Pages 30-37
DOI: 10.18775/ijom.2757-0509.2020.12.4004
URL: http://dx.doi.org/10.18775/ijom.2757-0509.2020.12.4004

Selected Aspects of Information Security Management in Entities Performing Medical Activity

[1] Dominika Lisiak-Felicka, [2] Pawel Nowak, [3] Maciej Szmit
[1,2] Department of Computer Science in Economics, University of Lodz, Poland
[3] Department of Computer Science, University of Lodz, Poland

Abstract: The article is devoted to the issues related to an information security management in medical entities. The healthcare entities have been amongst the prime targets for hackers for several years. According to the IBM report "The 2016 X-Force Cyber Security Intelligence Index" in 2015 most of the attacks were carried out against these entities. The years 2016 and 2017 also witnessed spectacular cyberattacks, for example: medical records breach of 3.3 million people because of an unauthorized access to a server in the US, some WannaCry ransomware attacks on the UK hospitals, some MongoDB Database Leaks in the US or NotPetya ransomware attacks in the US hospitals. Entities performing medical activity are processing personal data concerning health that is classified as a "sensitive data" and needs a special protection. The article presents the results of the survey – interviews with IT managers (or designated persons) in entities performing medical activity in Lodz Voivodeship in Poland. The aim of the research was analysis and evaluation of information security management in these entities. The interviews had been performed between December, 2017 and January, 2018. As the results of the research, the ways of information security management were identified (in particular such aspects as: characteristics of the information security teams, information security management system auditing, risk management, information security incidents, budgets for information security, training and the General Data Protection Regulation implementation). The paper also describes the types of information that should be protected in healthcare entities and characteristic of surveyed entities that subordinate to the local government of Lodz Voivodeship in Poland.

Keywords: Cybersecurity, Entities performing medical activity, Hospitals, Information security, Information security management

1. Introduction

In Poland the issues related to information security management in entities performing medical activities are important in the context of:

- personal data protection, including sensitive data (especially in connection with an implementation of the General Data Protection Regulation (GDPR, 2016),
- implementation of the patient's right regarding access to medical records and medical confidentiality,
- protection of personal rights that are listed in article 23 of The Civil Code (Lisiak-Felicka, Zajdel-Całkowska, Zajdel, 2017).

1.1 Health information

Entities performing medical activities are processing health information. There is a lot of definitions of this concept. For example, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR, 2016), (Voight, von dem Bussche, 2017) defines "data concerning health" as a personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Furthermore, standard ISO/IEC 27779:2016 defines "personal health information" as information about an identifiable person that relates to the physical or mental health of the individual. It may include:

- information about the registration of the individual for the provision of health services,
- information about payments or eligibility for health care in respect to the individual,
- a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes,
- any information about the individual that is collected in the course of the provision of health services to the individual,
- information derived from the testing of examination of a body part or bodily substance,
- identification of a person (e.g. a health professional) as provider of healthcare to the individual.

The standard gives guidelines for organizational information security standards and information security management practices, including the selection, implementation and management of controls taking into consideration the organization's information security risk environment (ISO 27799:2016). It also specifies types of health information that should be protected. Figure 1 presents these types. It should be noticed that this standard applies to health information in all its aspects (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing, writing on paper, electronically) and whatever means are used to transmit it (by hand, fax, computer networks, post).

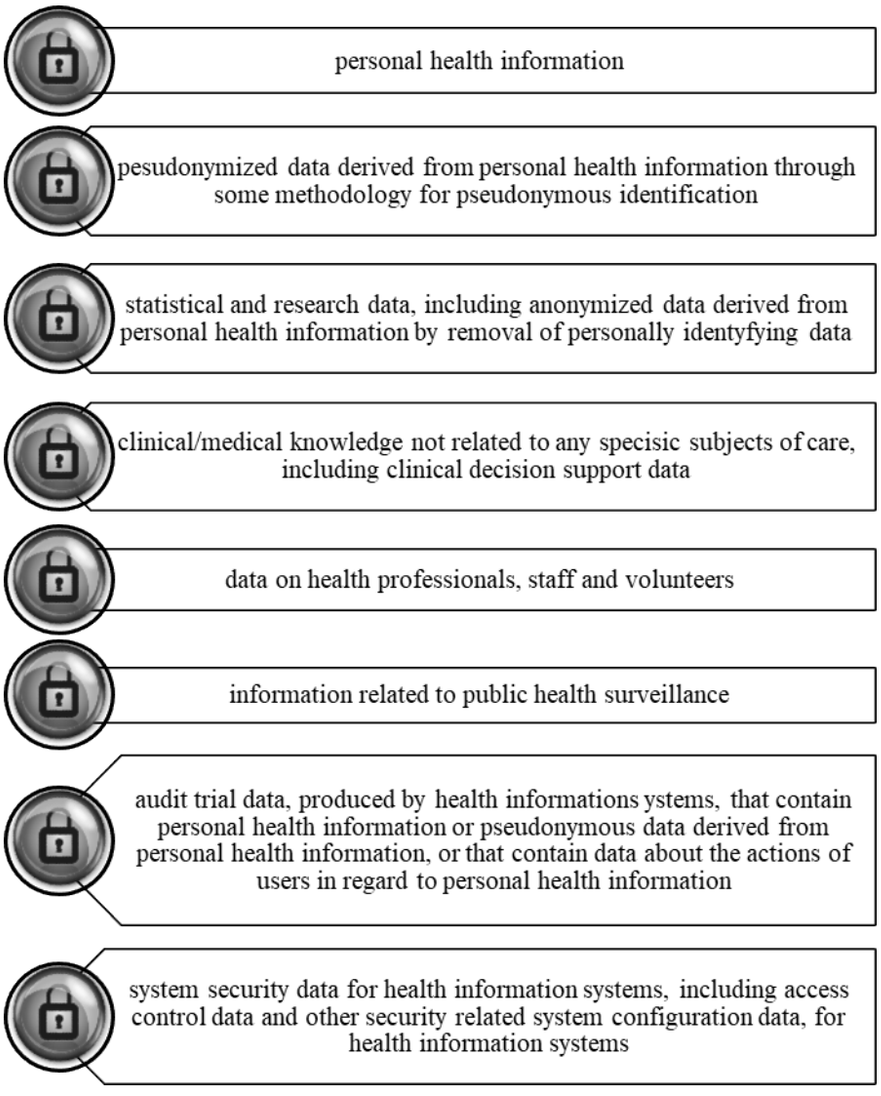

Figure 1: Types of health information that should be protected according to ISO/IEC 27799:2016.
Source: own preparation on the basis of the ISO/IEC 27799.

Issues related to the management of information security in medical entities are the subject of many surveys conducted in many countries (Chen et al., 2010), (Hou, Gao, Nicholson 2018), (Mehraeen, Ayatollahi, Ahmadi, 2016), (Sánchez-Henarejos et al., 2014), (Woo-Sung, 2010), (Zammani, Razali, 2016), (Zarei, Sadoughi 2016).

1.2 Information Security Incidents in Medical Entities

According to the IBM report "The 2016 X-Force Cyber Security Intelligence Index" in 2015 most of the attacks were carried out against medical entities (IBM, 2016). The media are increasingly informing about attacks on hospitals. Some examples of spectacular cyberattacks from years 2016 and 2017, are indicated below:

- In May, 2016 there was a breach of medical records of 3.3 million people in the US. Cybercriminal gained unauthorized access to a server that containing personal data (Abel, 2016);
- In June, 2016 an Arizona-based healthcare provider, disclosed a cyberattack that had compromised the records of 3.62 million patients (Alltucker, 2016);
- In February, 2017 due to a misconfigured MongoDB data on almost 80,000 individuals was exposed on the Internet at Emory Healthcare (Haber, 2017);
- In May, 2017 there were some WannaCry ransomware attacks. A massive ransomware attack had shut down work at 16 hospitals across the United Kingdom (Brandom, 2017);
- In June, 2017 there was a NotPetya ransomware attacks in the US hospitals (Glaser, 2017).

In Poland there were also some spectacular attacks, for example leak of sensitive data on approximately 50,000 patients of the Independent Public Health Care Center in Koło (Heartle, 2017) or data leak of hundreds of patients from dozens of hospitals on the server of external company serving hospitals (Maj, 2017).

1.3 The Subject of The Research

The organization and scope of the healthcare system operation in Poland follows directly from Article 68 of the Constitution of the Republic of Poland of 2nd April 1997 (Constitution of RP, 1997) that provides all citizens with health protection through equal access to public funded healthcare services. The main load of healthcare organizations falls on local government units (including at the level of primary healthcare, outpatient specialist care and hospital care), and the basis for its financing are public funds (e.g. health contributions of citizens through the National Health Fund, state budget funds and own resources of local government units). The method of financing health services results, among others, from the Act of 27th July, 2004 on health care services financed from public funds (UoSOZ, 2004), the Act of 15th April, 2011 on medical activities (UoDL, 2011) and Acts of local government: the Act of 8th March, 1990 about the municipal local government (UoSG, 1998), the act of 5th June 1998 on the district local government (UoSP), the act of 5th June 1998 on the voivodeship local government (UoSW, 1998). Local government of the Lodz Voivodeship implementing its statutory tasks (UoSW, 1998), at the end of June 2017 launched 10 multi-department hospitals (within which there are 3 care and treatment facilities), Voivodeship Center of Occupational Medicine, Voivodeship Emergency Medical Station and Independent Public Health Care Center PABIAN-MED. There were 11,655 people employed in these entities (including: 1297 doctors, 4,191 nurses and 417 midwives). The Statistical Bulletin of the Ministry of Health shows that subordinate institutions of the local government of the Lodz Voivodeship provides more than half of hospital beds (6,248 of 12,573 (CSIOZ, 2017, p. 72) in the region, 295 places in day wards and 40 dialysis stations (Regional Information Service, 2018). This means that with an average occupancy of 47.3 people per bed in the region (CSIOZ, 2017, p. 65), it gives about 250,000 patients in the hospital wards, and together with hospital outpatient clinics and emergency medical services, over 1.5 million people whose personal data (including sensitive data) go to IT systems operating in healthcare entities subordinate to the local government of the Lodz Voivodeship. Figure 2 presents all entities subordinate to the local government of the Lodz Voivodeship.

Figure 2: Entities subordinate to the local government of the Lodz Voivodeship.
Source: own preparation on the basis of Regional Information (Regional Information Service, 2018).

2. Method of The Research

The aim of the research was analysis and evaluation of selected aspects of information security management in entities performing medical activity. The research has been conducted using a CATI (Computer Assisted Telephone Interview) method between December, 2017 and January, 2018. The questions were related to:

- characteristics of the information security teams,
- Information Security Management System (ISMS) auditing,
- risk management,
- information security incidents,
- budgets for information security,
- training,
- General Data Protection Regulation implementation (O'Connor, Rowan, Lynch, Heavin, 2017)
- number of employees in particular entities.

Among 13 entities, 10 agreed to participate in the research. Due to the anonymous survey and respondents' requests for data anonymization in the next section names of units are omitted.

3. Results

Among 10 entities, 8 have special information security teams. In the other 2 units there is only one person who is responsible for information security. These teams consist of people from different departments, such as:

- IT department, HR and training department, maintenance department,
- IT department, HR department, maintenance department,
- IT department, HR department, administration department,
- information security administrator, personal security administrator, technical security administrator, IT security administrator,
- HR department, administrative department, technical department,
- HR department, operating department, auditors,
- information security administrator, IT department, HR department, administrative and technical department,
- IT department, medical dispatcher, occupational health and safety, public procurement staff, secretary, external person - GDPR, additional persons are appointed depending on the issues.

All of the entities conduct information security audits. A frequency of audits is as follows:

- once a year – 5 indications,
- minimum once a year – 3 indications,
- quarterly and temporarily as needed – 1 indication,
- according to the schedule – 1 indication.

The audits are external and internal (4 indications), only external (4 indications) and only internal (2 indications). External audits are related to the ISMS certification. Audits are conducted by information security administrator with participation of other employees, internal auditors and auditors from the marshal office. The audit teams also consist of employees from the following departments: medical statistics, accounting, quality control, organizing. One entity specified that there are minimum 2 auditors from each department (defined in the information security policy) in the team, the IT department employee is an accompanying person, and other people are involved in the audit team too. Next part of interview focused on the issues related to information security incidents. A big discrepancies in numbers (due to the problems with the classification of incidents) can be observed in the respondents' answers. Three entities declared that there have been no incidents for the last 12 months, the others declared that different numbers of incidents (from 1 to almost 1700) were recorded. Table 1 presents the respondents' answers.

Table 1: Numbers of information security incidents in the surveyed entities.

Numbers of incidents	Numbers of indications
None	3
1	1
2-3	1
5-6	1
a few	1
800-900	1
around 1000	1
around 1700	1

Source: own research.

Only 2 units reported information security incidents to the police and prosecutors office. In the opinion of the other respondents, there was no need to report incidents, because they concerned to minor offenses, failures, and oversights. As the consequences of incidents occurred, the respondents indicated implementation of corrective actions, training of employees and increased workload of IT specialists. In the 8 entities the risk estimation process was implemented. They use an author's methods adapted to the needs of the entity, a method developed by external company (for certification) or a method prepared by marshal office. Other units are working on the implementation of the risk estimation

method. Respondents had many problems with questions regarding the budget for information security. Four of respondents declared that it is 0.1-0.2% of all entity budget. Others respondents were unable to specify the annual amount allocated for information security. However, all agreed that the particular budgets for information security are insufficient. Six respondents described the allocation of the budget. Funds are spent on:

- hardware, training, maintenance,
- training, auditors training
- training, software hardware,
- software, training, hardware, adjustment of documentation, physical security equipment,
- software,
- training, physical security equipment.

Training in information security, information system security and personal data protection have been conducted in the all entities. Two respondents declared that there is a problem with the training of all employees. Entities conduct training employees when they hiring them and also periodic training (in 6 entities) is carried out. Four of the entities declared that they plan to conduct training in the near future. An external and an internal training were conducted in all units, but external were mostly for the management, auditors and information security administrators. Respondents were asked about the General Data Protection Regulation implementation. Answering the question about determining the degree of preparation for introducing changes resulting from the GDPR, six respondents defined this grade at 3, three respondents defined this grade at 2, and one of the respondents indicated the lowest degree. As the biggest problems in implementation they indicated: lack of financial and human resources, barriers of awareness and ambiguity and fluctuation of the law. The last question concerned to a size of surveyed units in terms of the number of employed persons. Figure 3 presents the numbers of employees in surveyed entities.

Figure 3: Numbers of employees in the entities. Source: own research.

4. Discussion and Conclusion

It could be concluded that the ways of information security management (in terms of the surveyed aspects) are different in different surveyed entities. The main concern is ensuring of information security by one person (there were two cases among surveyed entities). It is impossible to individually operate correctly in entities with several hundred or a thousand employees. Particularly noteworthy is also the large discrepancy in the numbers of information security incidents. It may be a result of inappropriate classification of incidents or different interpretation of the incident definition. It is also necessary to devote adequate resources from the budgets to manage information security. All respondents declared that the available financial resources are not enough. These resources should be allocated not only for software, hardware and training, but also for support of IT administrators. In the respondents' opinion the management staffs usually have a problem with understanding that teams have too few members and the scope of duties is increasing (monitoring responsibilities are increasing, administrator's work is needed non-stop, often there is a need for an immediate reaction to the incident). In order to ensure proper protection, it is necessary to allocate financial resources for the extension of information security teams. The lack of efficient information security management in medical entities may contribute to the incidents occurrence in future. The results of the research are consistent with the results of 2018 HIMSS

Cybersecurity Survey (HIMMS, 2018) in which the biggest barriers for cybersecurity incidents management is lack of appropriate cybersecurity personnel (52.4%) and lack of financial resources (46.6%). In the context of further research, survey in the entities performing medical activity from the other voivodeships is planned.

References

- Abel R. (2016). Newkirk medical records breach impacts 3.3M, Blue Cross Blue Shield customers affected. Retrieved 20.08.2018 from https://www.scmagazine.com/home/news/newkirk-medical-records-breach-impacts-3-3m- blue-cross-blue-shield-customers-affected/.
- Alltucker K. (2016). Banner Health cyberattack breaches up to 3.7M records. Retrieved 20.08.2018 from https://eu.usatoday.com/story/news/nation-now/2016/08/03/banner-health-cyberattack-breaches-reords/88040778/.
- Brandom R.(2017). UK hospitals hit with massive ransomware attack. Retrieved 20.08.2018 from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack- wannacry-bitcoin).
- Chen YP., Hsieh SH., Cheng PH., Chien TN., Chen HS., Luh JJ., Lai JS., Lai FP., Chen SJ.(2010). An Agile Enterprise Regulation Architecture for Health Information Security Management. Telemedicine Journal and E-health. Volume: 16, Issue: 7. Crossref
- Constitution of RP (1997). Constitution of the Republic of Poland of 2nd April, 1997. Retrieved 20.08.2018 from http://www.sejm.gov.pl/prawo/konst/polski/kon1.htm, last accessed 2018/03/30.
- CSIOZ (2017). Statistical Bulletin of the Ministry of Health. Retrieved 20.08.2018 from https://www.csioz.gov.pl/fileadmin/user_upload/statystyka/biuletyn_2017_5a2e86b48fba 0.pdf.
- GDPR (2016) - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved 20.08.2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
- Glaser A. (2017). U.S. hospitals have been hit by the global ransomware attack. Retrieved 20.08.2018 from https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us- hackers-nsa-hospitals.
- Haber M. (2017). The Fallout from MongoDB Breaches. Retrieved 20.08.2018 from https://www.beyondtrust.com/blog/fallout-mongodb-breaches/.
- Haertle A. (2017). Wyciek danych wrażliwych 50 tysięcy pacjentów polskiego szpitala. Retrieved 20.08.2018 from https://zaufanatrzeciastrona.pl/post/wyciek-danych- wrazliwych-50-tysiecy-pacjentow-polskiego-szpitala/.
- HIMMS (2018). 2018 HIMSS Cybersecurity Survey. Retrieved 20.08.2018 from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.
- Hou Y., Gao P., Nicholson B. (2018). Understanding organizational responses to regulative pressures in information security management: The case of a Chinese hospital. Technological Forecasting and Social Change. Volume: 126. Crossref
- IBM (2016). 2016 Cyber Security Intelligence Index. Retrieved 20.08.2018 from http://www-03.ibm.com/security/data-breach/cyber-security-index.html.
- ISO 27799:2016 Health informatics - Information security management in health using ISO/IEC 27002.
- Lisiak-Felicka D., Nowak P.: Wybrane aspekty zarządzania bezpieczeństwem informacji w podmiotach prowadzących działalność leczniczą, Przedsiębiorczość i Zarządzanie, Społeczna Akademia Nauk, Łódź-Warszawa (in print), (2018).
- Lisiak-Felicka D., Zajdel-Całkowska J., Zajdel R. (2017): Wybrane aspekty zarządzania bezpieczeństwem informacji w podmiotach prowadzących działalność leczniczą, Przedsiębiorczość i Zarządzanie, tom XVIII, zeszyt 4, część 2, Społeczna Akademia Nauk, Łódź-Warszawa.
- Maj M. (2017). Dane setek pacjentów na serwerze zewnętrznej firmy obsługującej szpitale. Retrieved 20.08.2018 from https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali- wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/.
- Mehraeen E., Ayatollahi H., Ahmadi M. (2016). Health Information Security in Hospitals: the Application of Security Safeguards. Acta informatica medica, 24(1). Crossref
- O'Connor Y., Rowan W., Lynch L., Heavin C. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. Procedia Computer Science. Volume: 113. Crossref
- Regional Information Service (2018). Jednostki podległe, Retrieved 20.08.2018 from http://www.zdrowie.lodzkie.pl/zadania-departamentu/jednostki-podlegle.
- Sánchez-Henarejos A., Fernández-Alemán JL., Toval A., Hernández-Hernández I., Sánchez-García AB., Carrillo de Gea JM. (2014). A guide to good practice for information security in the handling of personal health data by health personnel in ambulatory care facilities. Aten Primaria 46(4). Crossref
- UoDL (2011). Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U.2011 Nr 112).

- UoSG (1998). Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.1990 Nr 16).
- UoSOZ (2004). Ustawa z dnia 27 lipca 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U.2004 Nr 210).
- UoSP (1998). Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. 1998 Nr 91).
- UoSW (1998). Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz.U. 1998 Nr 91).
- Voight P., von dem Bussche A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer International Publishing AG, https://doi.org/10.1007/978-3-319-57959-7. Crossref
- Woo-Sung Park, Sun-Won Seo, Seung-Sik Son, Mee-Jeong Lee, Shin-Hyo Kim, Eun-Mi Choi, Ji-Eon Bang, Yea-Eun Kim, Ok-Nam Kim (2010). Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds. Healthcare Informatics Research, 16(2). Crossref
- Zammani M., Razali R.(2016). Information Security Management Success Factors, Advanced Science Letters. Volume: 22, Issue: 8. Crossref
- Zarei J., Sadoughi F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. Risk management and health policy. Vol. 9. Crossref