ZESZYTY NAUKOWE UNIWERSYTETU PRZYRODNICZO-HUMANISTYCZNEGO W SIEDLCACH Nr 126
Seria: Administracja i Zarządzanie (53) 2020
pl ISSN 2082-5501

THE FINANCING OF INFORMATION SECURITY MANAGEMENT IN ENTITIES PERFORMING MEDICAL ACTIVITIES

FINANSOWANIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PODMIOTACH WYKONUJĄCYCH DZIAŁALNOŚĆ LECZNICZĄ

https://doi.org/10.34739/zn.2020.53.01

Dominika **Lisiak-Felicka**[1], Paweł A. **Nowak**[2], Maciej **Szmit**[3], Radosław **Zajdel**[4]

[1] Poland, University of Łódź, Faculty of Economics and Sociology
dominika.lisiak@uni.lodz.pl, ORCID: 0000-0001-8451-4268

[2] Poland, University of Łódź, Faculty of Economics and Sociology
pawel.nowak@uni.lodz.pl, ORCID: 0000-0002-9681-0627

[3] Poland, University of Łódź, Faculty of Management
maciej.szmit@uni.lodz.pl, ORCID: 0000-0002-6115-9213

[4] Poland, University of Łódź, Faculty of Economics and Sociology
radoslaw.zajdel@uni.lodz.pl, ORCID: 0000-0002-1654-8957

JEL Classification Codes: M10

Abstract: All healthcare organizations process “sensitive data” that needs special protection. To ensure an appropriate level of security for this data, it is necessary to allocate adequate financial resources for security measures. The exploratory aim of the research here is the recognition of the current state of information security management systems in selected entities performing medical activities. An analysis and evaluation of these systems and the financing of information security were conducted. The methods and techniques used in the research are Computer Assisted Telephone Interviews, literature studies, and a questionnaire survey with applications for access to public information. The subjects of the research were medical entities subordinate to the local governments of three Polish voivodeships (Łódź, Świętokrzyskie and Pomeranian). The research was conducted between 2017 and 2018. Research findings show that the surveyed entities did not properly manage information security and did not allocate adequate financial resources to ensure information security. The lack of efficient information security management in medical entities may entail negative consequences in the future.
Keywords: information security management, sensitive data, entities performing medical activities, financing, data security breaches

Abstract: Wszystkie organizacje opieki zdrowotnej przetwarzają „dane wrażliwe”, które wymagają specjalnej ochrony. W celu zapewnienia właściwego poziomu bezpieczeństwa tych danych, konieczne jest przeznaczenie odpowiednich środków finansowych. Celem poznawczym badań jest rozpoznanie istniejącego stanu systemów zarządzania bezpieczeństwem informacji w wybranych podmiotach wykonujących działalność leczniczą. Przeprowadzono analizę i ocenę tych systemów oraz finansowania bezpieczeństwa informacji. W badaniach wykorzystano następujące metody i techniki: wspomagany komputerowo wywiad telefoniczny, studia literaturowe i ankietę z wnioskiem o udostępnienie informacji publicznej. Przedmiotem badań były podmioty medyczne podległe samorządom trzech polskich województw (łódzkie, świętokrzyskie, pomorskie). Badanie było prowadzone w latach 2017-2018. Wyniki badania pokazują, że badane podmioty nieprawidłowo zarządzały bezpieczeństwem informacji i nie przeznaczały odpowiednich środków finansowych na zapewnienie bezpieczeństwa informacji. Brak efektywnego zarządzania bezpieczeństwem informacji w podmiotach medycznych może mieć wpływ na wystąpienie incydentów w przyszłości.
Słowa kluczowe: zarządzanie bezpieczeństwem informacji, dane wrażliwe, podmioty wykonujące działalność leczniczą, finansowanie, naruszenia bezpieczeństwa danych

Introduction

Information security management in entities performing medical activities is a huge challenge. These organizations process personal data concerning health that is classified as “sensitive data” and needs special protection. To ensure adequate security, it is necessary to ensure sufficient financial resources. It is also necessary to take into account the amount of financial resources that probably could be used in the case of a data protection breach. In 2018, the ‘Cost of a

Data Breach Study. Global Overview' report showed that the average total cost of a data breach had risen from $3.62 to $3.86 million, an increase of 6.4%. The average cost for each lost record rose from $141 to $148, an increase of 4.8%, and the average size of the data breaches in this research increased by 2.2%. It also noted that heavily regulated industries, such as healthcare and financial organizations, have a per capita data breach cost substantially higher than others. The per capita cost of a data breach in healthcare is approximately $408 per record, significantly more than in the finance industry, which can cost $206 per record, and the public sector, which can cost $75 per record (Ponemon Institute, 2018, Herjavec Group, 2019).

Literature review

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

Entities performing medical activities process health information. There are many definitions of this concept; however, Appari and Johnson (2010) define health information as all the information that could be applied to health and healthcare.

For example, the ISO/IEC 27779:2016 standard 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 an individual for the provision of health services,
- information about payments or eligibility for health care in respect to an individual,
- a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes,
- any information about an individual that is collected in the course of the provision of health services to the individual,
- information derived from the testing or examination of a body part or bodily substance,
- the identification of a person (e.g., a health professional) as a provider of healthcare to an 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).

Furthermore, 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) (EU, 2016), defines "data concerning health" as 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.

GDPR has changed the approach to the personal data protection system, introduced a number of significant changes and unified the rules on the protection of personal data in all EU countries. GDPR specified some important obligations that should be implemented in all entities processing personal data (O'Connor et al., 2017; Voight, von dem Bussche, 2017).

This article concerns the issues related to information security management in entities performing medical activities from Poland, so it is also important to indicate the legal conditions, especially: personal data protection, including sensitive data (especially in connection with the implementation of GDPR), implementation of the patient's right regarding access to medical records and medical confidentiality and protection of personal rights that are listed in article 23 of The Civil Code (Lisiak-Felicka et al., 2017; Lisiak-Felicka, Nowak, 2018).

Sensitive data that are processed in entities performing medical activities are exposed to many attacks conducted by cybercriminals. Healthcare information is an attractive target for cyber attackers. In the case of an absence of adequate information security, such an incident may involve high costs, for example, recovering lost data, order additional work for administrators or an IT company, and in the case of a ransomware attack, when the unit did not have a copy of the data, also the costs of purchasing access to the system. Healthcare entities have been amongst the prime targets for hackers for several years. Among the spectacular attacks in recent years, one can distinguish the following:

- In February 2017, due to a misconfigured MongoDB, data on almost 80,000 individuals at Emory Healthcare was exposed on the Internet (Haber, 2017);
- In May 2017, there were several WannaCry ransomware attacks. A massive ransomware attack shut down work at 16 hospitals across the United Kingdom (Brandom, 2017);

- In June 2017, there was the NotPetya ransomware attack in US hospitals (Glaser, 2017);
- In November 2017, a hacker gained access to an Oklahoma State University Center for Health Sciences network. He accessed folders containing Medicaid billing data and had access to nearly 280,000 Medicaid patient records. After the breach, the folders were removed from the network, and third-party access was terminated the next day (Davis, 2018a);
- In Poland, there were also some spectacular attacks, for example, a leak of sensitive data on approximately 50,000 patients of the Independent Public Health Care Center in Koło (Haertle, 2017) or data leak of hundreds of patients from dozens of hospitals on the server of an external company serving hospitals (Maj, 2017).

The predominant incidents in 2018 were ransomware, misconfigured cloud storage buckets, and phishing emails. As a sample of incidents, one can distinguish the following:

- From May 2017 to January 2018, the data of 33,000 patients of BJC HealthCare was available on the Internet for eight months after the St. Louis-based provider misconfigured one of its servers (Davis, 2018b).
- In June 2018, The Fetal Diagnostic Institute of the Pacific in Haiti was hit by a ransomware attack that potentially breached the data of 40,800 patients. They were able to restore data from backups; and with help from a cybersecurity firm, they wiped the virus from the infected server (Davis, 2018c).
- In October 2018, the files of an estimated 75,000 individuals were accessed in a breach of the Healthcare.gov site's Affordable Care Act enrolment system, according to the Centers for Medicare and Medicaid Services. They implemented additional security measures (Morse, 2018).

This paper is a revised and expanded version of a paper entitled Selected Aspects of Information Security Management in Entities Performing Medical Activity presented at Economic and Social Development Conference (Moscow, 18-19 October 2018) (Lisiak-Felicka et al., 2018).

Methodology and theoretical basis

The research was divided into three parts. Firstly, a Computer Assisted Telephone Interview (CATI) method was used. The survey was conducted between December 2017 and January 2018. The questions were related to: the characteristics of the information security teams, Information Security Management System (ISMS) auditing, risk management, information security incidents, budgets for information security management, training, the GDPR implementation, and the number of employees in particular entities. Interviews were conducted in entities performing medical activities subordinate to the local government of the Łódź voivodeship.

The organization and scope of the healthcare system's operations in Poland follow directly from Article 68 of the Constitution of the Republic of Poland of 2 April 1997 (Constitution of RP, 1997) which provides all citizens with health protection through equal access to publicly funded healthcare services. The main burden 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 is public funds (e.g., the health contributions of citizens through the National Health Fund, state budget funds, and local government units' own resources). The methods of financing health services result from, among others, the Act of 27 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 8 March 1990 about municipal local government (UoSG, 1998), the act of 5 June 1998 on district local government (UoSP), and the act of 5 June 1998 on voivodeship local government (UoSW, 1998). A list of entities performing medical activities subordinate to the local government of the Łódź voivodeship is shown in the Figure 1.

Following this, a statistical analysis of data from the Statistical Bulletin of the Ministry of Health was conducted. The report is issued by the Healthcare Information Systems Center and contains detailed information about diseases, as well as information on the number of hospitals and medical personnel according to the state for particular years.

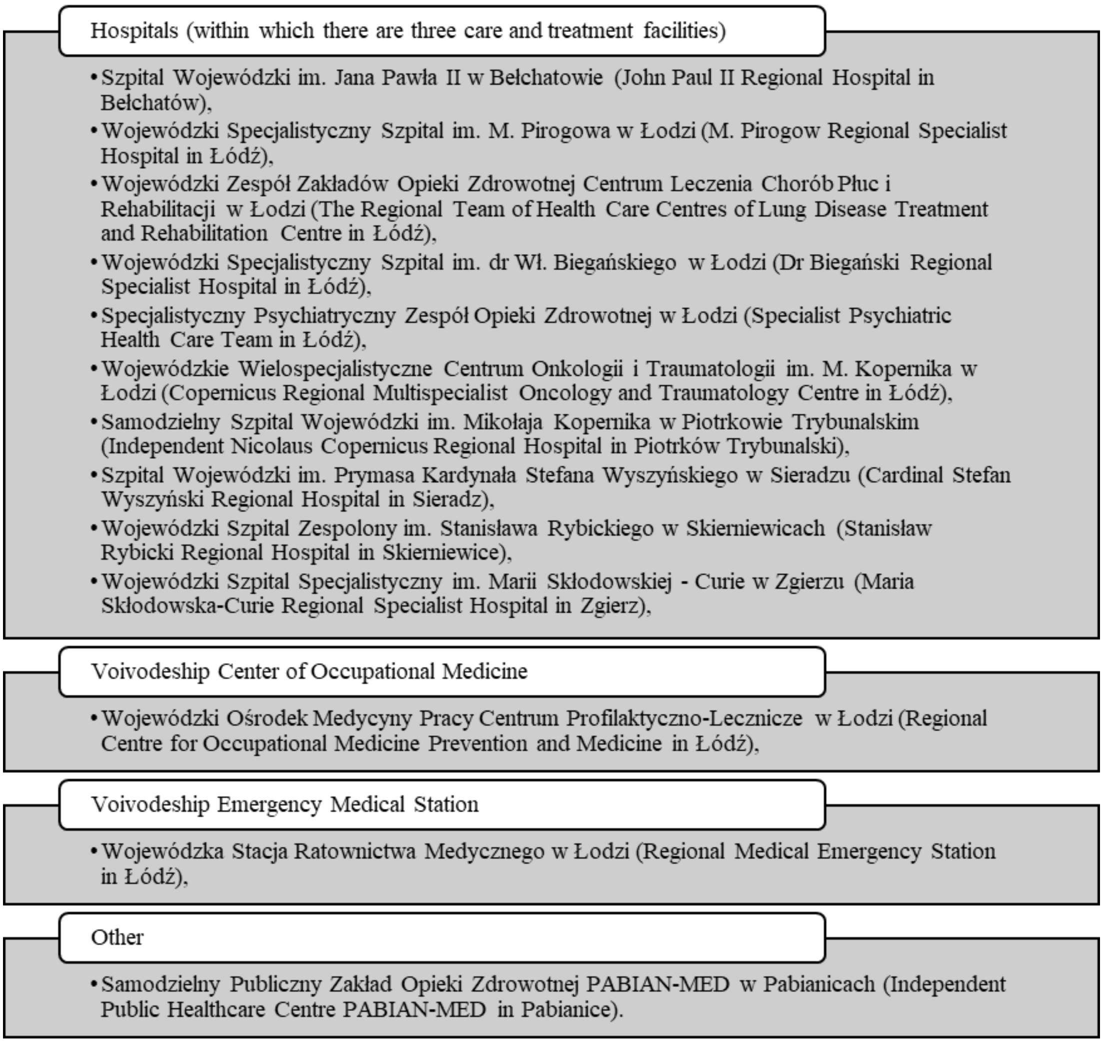
Finally, between November and December 2018, applications for access to public information about financing information security in entities performing medical activity were sent to 20 hospitals from three voivodeships (Łódź, Pomeranian, Świętokrzyskie), see Figure 2.

Given the extent of the scope of research, it was assumed that institutions of interest would be those whose founding body is the voivodeship local government. Because hospitals from the Łódź voivodeship had been invited to take part in the first part of the research, the applications for access to public information were sent to them first.

However, in order to check whether the described phenomenon has a regional nature or is a broader problem of research, entities performing medical activities subordinate to self-governments of the Świętokrzyskie and Pomeranian voivodeships were also included in the study.

The choice of these voivodeships was not accidental. These regions are characterized by economic and demographic indicators that are different from the Łódź voivodeship. The Świętokrzyskie voivodeship together with the Subcarpathian, Lublin, Podlaskie and Warmian-Masurian voivodeships belong to the "Eastern Poland" group of voivodeships. They are covered by structural EU assistance resulting from the deteriorating demographic situation and indicators of economic development significantly lower than average in Poland.

The Pomeranian voivodeship, together with Greater Poland, Mazovian and Silesian voivodeships, belongs to a region with demographic and economic indicators that are significantly higher than the national average. Assuming that the Pomeranian voivodeship is located on the upper part of the scale, and the Świętokrzyskie voivodeship on the lower part, the Łódź voivodeship is located exactly in the middle. Simultaneously, and of great importance, the local government authorities in all of the surveyed voivodeships declare ongoing activities for the well-being of residents, which includes increasing both the availability of health services and expenditure for the development of public e-services in the area of health.



Hospitals (within which there are three care and treatment facilities)

- Szpital Wojewódzki im. Jana Pawła II w Bełchatowie (John Paul II Regional Hospital in Bełchatów),
- Wojewódzki Specjalistyczny Szpital im. M. Pirogowa w Łodzi (M. Pirogow Regional Specialist Hospital in Łódź),
- Wojewódzki Zespół Zakładów Opieki Zdrowotnej Centrum Leczenia Chorób Płuc i Rehabilitacji w Łodzi (The Regional Team of Health Care Centres of Lung Disease Treatment and Rehabilitation Centre in Łódź),
- Wojewódzki Specjalistyczny Szpital im. dr Wł. Biegańskiego w Łodzi (Dr Biegański Regional Specialist Hospital in Łódź),
- Specjalistyczny Psychiatryczny Zespół Opieki Zdrowotnej w Łodzi (Specialist Psychiatric Health Care Team in Łódź),
- Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi (Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź),
- Samodzielny Szpital Wojewódzki im. Mikołaja Kopernika w Piotrkowie Trybunalskim (Independent Nicolaus Copernicus Regional Hospital in Piotrków Trybunalski),
- Szpital Wojewódzki im. Prymasa Kardynała Stefana Wyszyńskiego w Sieradzu (Cardinal Stefan Wyszyński Regional Hospital in Sieradz),
- Wojewódzki Szpital Zespolony im. Stanisława Rybickiego w Skierniewicach (Stanisław Rybicki Regional Hospital in Skierniewice),
- Wojewódzki Szpital Specjalistyczny im. Marii Skłodowskiej - Curie w Zgierzu (Maria Skłodowska-Curie Regional Specialist Hospital in Zgierz),

Voivodeship Center of Occupational Medicine

- Wojewódzki Ośrodek Medycyny Pracy Centrum Profilaktyczno-Lecznicze w Łodzi (Regional Centre for Occupational Medicine Prevention and Medicine in Łódź),

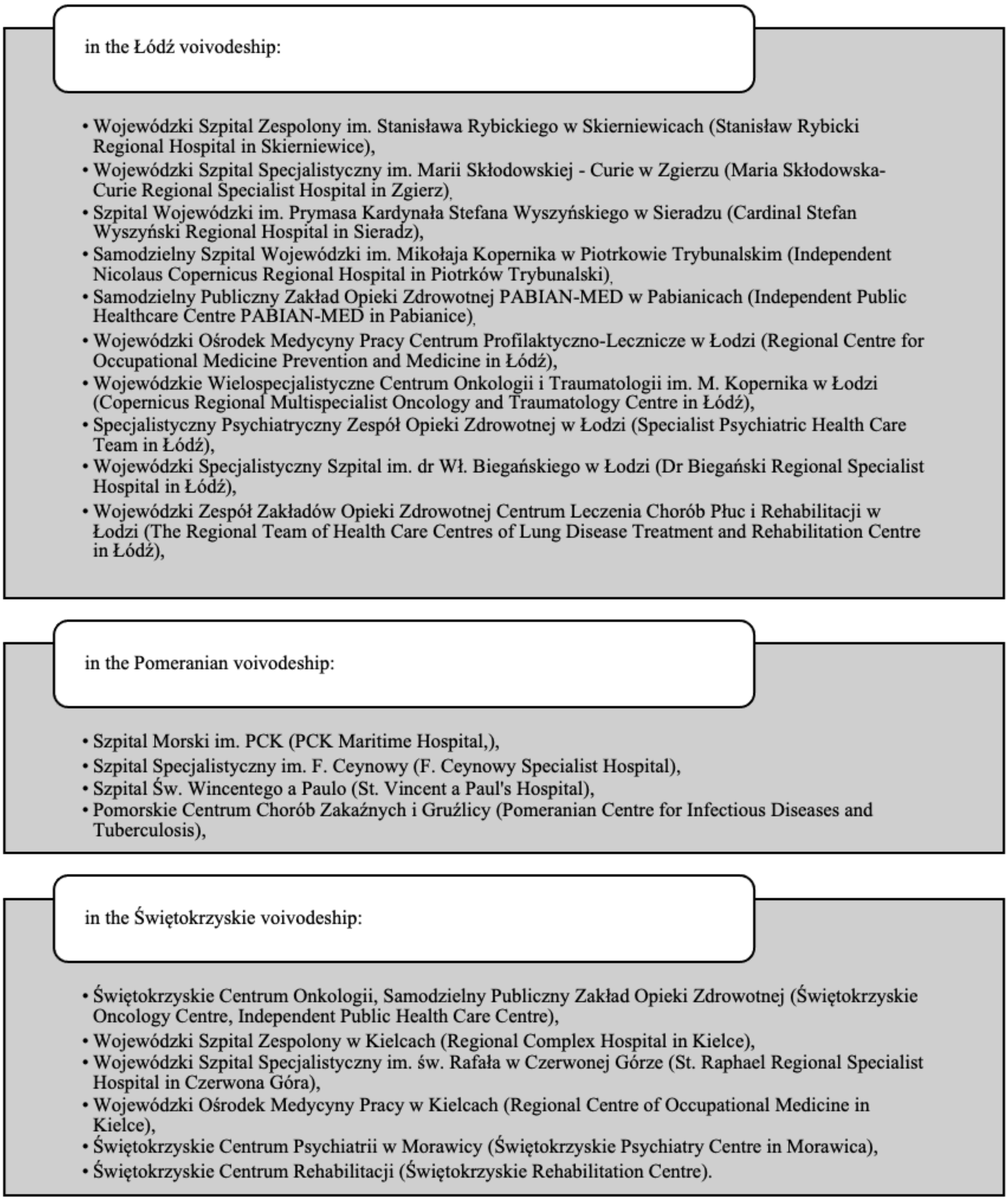
Voivodeship Emergency Medical Station

- Wojewódzka Stacja Ratownictwa Medycznego w Łodzi (Regional Medical Emergency Station in Łódź),

Other

- Samodzielny Publiczny Zakład Opieki Zdrowotnej PABIAN-MED w Pabianicach (Independent Public Healthcare Centre PABIAN-MED in Pabianice).

Figure 1. List of entities performing medical activities subordinate to the local government of the Łódź voivodeship
Source: own preparation on the basis of the Regional Information Service (2018).



in the Łódź voivodeship:

- Wojewódzki Szpital Zespolony im. Stanisława Rybickiego w Skierniewicach (Stanisław Rybicki Regional Hospital in Skierniewice),
- Wojewódzki Szpital Specjalistyczny im. Marii Skłodowskiej - Curie w Zgierzu (Maria Skłodowska-Curie Regional Specialist Hospital in Zgierz),
- Szpital Wojewódzki im. Prymasa Kardynała Stefana Wyszyńskiego w Sieradzu (Cardinal Stefan Wyszyński Regional Hospital in Sieradz),
- Samodzielny Szpital Wojewódzki im. Mikołaja Kopernika w Piotrkowie Trybunalskim (Independent Nicolaus Copernicus Regional Hospital in Piotrków Trybunalski),
- Samodzielny Publiczny Zakład Opieki Zdrowotnej PABIAN-MED w Pabianicach (Independent Public Healthcare Centre PABIAN-MED in Pabianice),
- Wojewódzki Ośrodek Medycyny Pracy Centrum Profilaktyczno-Lecznicze w Łodzi (Regional Centre for Occupational Medicine Prevention and Medicine in Łódź),
- Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi (Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź),
- Specjalistyczny Psychiatryczny Zespół Opieki Zdrowotnej w Łodzi (Specialist Psychiatric Health Care Team in Łódź),
- Wojewódzki Specjalistyczny Szpital im. dr Wł. Biegańskiego w Łodzi (Dr Biegański Regional Specialist Hospital in Łódź),
- Wojewódzki Zespół Zakładów Opieki Zdrowotnej Centrum Leczenia Chorób Płuc i Rehabilitacji w Łodzi (The Regional Team of Health Care Centres of Lung Disease Treatment and Rehabilitation Centre in Łódź),

in the Pomeranian voivodeship:

- Szpital Morski im. PCK (PCK Maritime Hospital,),
- Szpital Specjalistyczny im. F. Ceynowy (F. Ceynowy Specialist Hospital),
- Szpital Św. Wincentego a Paulo (St. Vincent a Paul's Hospital),
- Pomorskie Centrum Chorób Zakaźnych i Gruźlicy (Pomeranian Centre for Infectious Diseases and Tuberculosis),

in the Świętokrzyskie voivodeship:

- Świętokrzyskie Centrum Onkologii, Samodzielny Publiczny Zakład Opieki Zdrowotnej (Świętokrzyskie Oncology Centre, Independent Public Health Care Centre),
- Wojewódzki Szpital Zespolony w Kielcach (Regional Complex Hospital in Kielce),
- Wojewódzki Szpital Specjalistyczny im. św. Rafała w Czerwonej Górze (St. Raphael Regional Specialist Hospital in Czerwona Góra),
- Wojewódzki Ośrodek Medycyny Pracy w Kielcach (Regional Centre of Occupational Medicine in Kielce),
- Świętokrzyskie Centrum Psychiatrii w Morawicy (Świętokrzyskie Psychiatry Centre in Morawica),
- Świętokrzyskie Centrum Rehabilitacji (Świętokrzyskie Rehabilitation Centre).

Figure 2. List of units participating in the survey
Source: own preparation on the basis of the research.

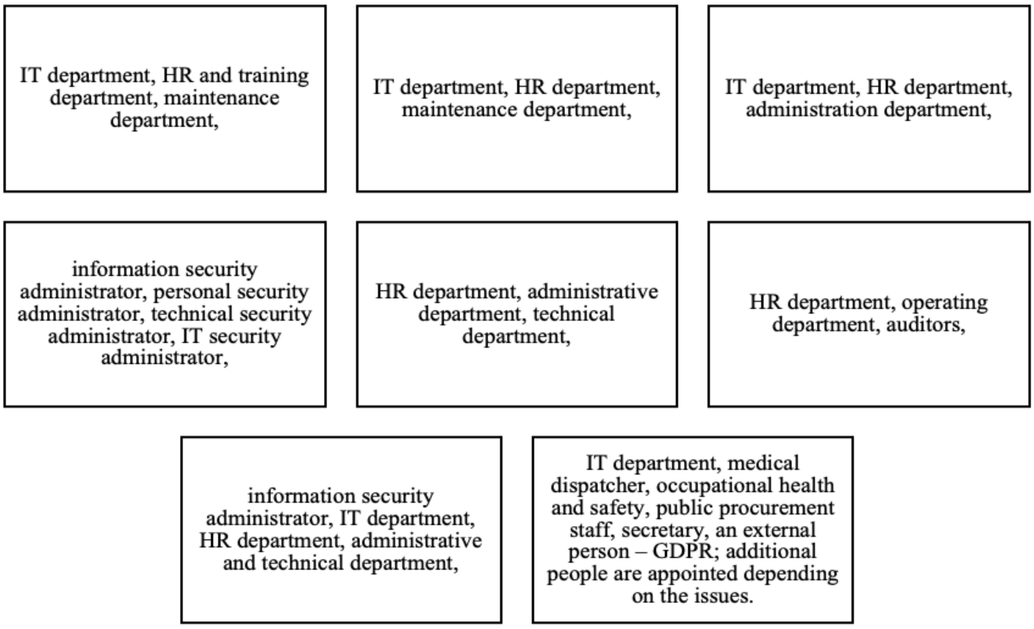
Results and discussion

The results of each research are presented in subsections.

Interviews

Among the 13 entities performing medical activities and which are subordinate to the local government of the Łódź voivodeship, 10 agreed to participate in the research. Due to the anonymity of the survey and the respondents' requests for data anonymization, in the next section, the names of the units are omitted.

Among the 10 participating 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 (see Figure 3).



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, an external person – GDPR; additional people are appointed depending on the issues.

Figure 3. Information security teams

Source: own preparation on the basis of the research.

All of the entities conduct information security audits. The frequency of audits is as follows: once a year – 5 indications, minimum once a year – 3 indications, quarterly and ad hoc– 1 indication, according to a 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. The audits are conducted by an information security administrator with the participation of other employees, internal auditors and auditors from the marshal's office. The audit teams also consist of employees from the following departments: medical statistics, accounting, quality control, and organization. One entity specified that there is a minimum of 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.

The next part of the interview focused on issues related to information security incidents. Big discrepancies in the numbers (due to problems with the classification of incidents) can be observed in the respondents' answers. Three entities declared that there had been no incidents in the last 12 months; the others declared that different numbers of incidents (from 1 to almost 1700) had been recorded.

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 the incident because they concerned minor offenses, failures, and oversights. As a consequence of the incidents, the respondents indicated they had implemented corrective actions, trained employees and increased the workload of their IT specialists.

In 8 entities, a risk estimation process had been implemented. They use existing methods adapted to the needs of the entity, a method developed by an external company (for certification), or a method prepared by the marshal's office. The other units are working on the implementation of a risk estimation method.

The respondents had many problems with questions regarding the budget for information security. Four of the respondents declared that it is 0.1-0.2% of the entity's entire budget. Other 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.

The respondents' answers to the above questions gave rise to more detailed analyses of the financing of information security management (see section Applications for access to public information).

Training in information security, information system security, and personal data protection had been conducted in all entities. Two respondents declared that there is a problem with the training of all employees. Entities train employees when they hire them, and periodic training is also carried out (in 6 entities). Four of the entities declared that they plan to conduct training in the near future. Internal and external training was conducted in all units, but external training was mostly for the management, auditors, and information security administrators.

The respondents were asked about the GDPR implementation. The regulation has been in force since the 25 May 2018. Before that day, all organizations from the EU that process personal data (also entities performing medical activities) were obliged to have implemented new requirements. The interviews were conducted before this date, so the aim of the research was also to verify if the units were prepared for the GDPR implementation.

Answering the question about determining the degree of preparation for introducing changes resulting from the GDPR, on a 5-point Likert scale six respondents defined this level at 3, three respondents put this level at 2, and one of the respondents indicated the lowest degree. Regarding the biggest problems in implementation, they indicated a lack of financial and human resources, barriers of awareness, and ambiguity and changes in the law.

The last question concerned the size of the surveyed units in terms of the number of employed people. Two entities have from 101 to 500 employees, six entities have between 501 and 1,000 employees, and two have between 1,001 and 2,000 employees.

Statistical data

As a part of the analysis, data about hospitals from the three surveyed voivodeships was collected, and descriptive statistics were conducted. According to the Statistical Bulletin of the Ministry of Health, in 2017 there were 930 stationary general hospitals in Poland with 181,548 beds. The number of patients treated during 2017 in all hospitals was 8,289,411. Table 1 presents information from the three surveyed voivodeships.

Table 1. Statistical data from the Statistical Bulletin of the Ministry of Health about the three surveyed voivodeships

Voivodeship	Number of stationary general hospitals	Number of beds	Number of beds per 10,000 people	The number of patients treated during the year
Łódź	64	12,569	50.8	580,523
Pomeranian	42	9,153	39.4	415,704
Świętokrzyskie	24	6,018	48.2	287,271

Source: own preparation on the basis of the Statistical Bulletin of the Ministry of Health (Ministry of Health, 2018).

The number of stationary general hospitals in the Łódź voivodeship is 7% of the total number of hospitals, in the Pomeranian voivodeship it is 5%, and in the Świętokrzyskie voivodeship, it is 3% of the total. The structure of the number of beds for the surveyed voivodeships is similar.

In 2017, the Łódź voivodeship had the most beds per 10,000 people, and this voivodeship also had the largest number of patients.

Below, the finances of local government independent public health care institutions are presented. The net income of 1032 such institutions amounted to 29,056 million zlotys and operating expenses were over 30,602 million zlotys. This means that the loss on operating activities in 2017 after taking into account other operating income (1,886 million zlotys) and costs (534 million zlotys) amounted to almost 194 million zlotys. Table 2 presents information from the three surveyed voivodeships.

Table 2. Statistical data from the Statistical Bulletin of the Ministry of Health about the three surveyed voivodeships – budgets

Voivodeship	Number of units	Incomes in million zlotys	Costs in million zlotys
Łódź	71	1.983	2.068
Pomeranian	36	457.000	471.000
Świętokrzyskie	77	1.569	1,668

Source: own preparation on the basis of the Statistical Bulletin of the Ministry of Health (Ministry of Health, 2018).

On the basis of the financial data, it can be noticed that all of the entities from the surveyed voivodeships had losses on operating activities; the largest in the Świętokrzyskie voivodeship (51% of total loss) and the smallest in the Pomeranian voivodeship (7% of total loss).

Applications for access to public information

Twenty applications were sent for access to public information about financing information security in entities performing medical activities; 10 responses were obtained (including one answer from a company of 4 hospitals). This part of the research was conducted due to the fact that, during the interviews, the respondents had a big problem in determining the percentage of expenditure on information security in the whole budget. Below, the information in relation to particular questions is presented.

Question 1. What is the budget for the entire facility for 2017? Table 3 presents the budgets of the surveyed units in 2017. The obtained data were not given explicitly, which hinders statistical analysis. However, it can be noticed that the surveyed entities had a budget between approximately 17 million zlotys to more than 450 million zlotys.

Table 3. Budgets of the surveyed units in 2017

Entity	Budget (in million zlotys)
Pomeranian Hospitals	450.4
Specialist Psychiatric Health Care Team in Łódź	46.9
Stanisław Rybicki Regional Hospital in Skierniewice	67.6
Regional Centre for Occupational Medicine Prevention and Medicine in Łódź	income: 16.6 costs: 17.4
Maria Skłodowska-Curie Regional Specialist Hospital in Zgierz	income: 114.6 costs: 114.5
Dr Biegański Regional Specialist Hospital in Łódź	151.5
Świętokrzyskie Oncology Centre, Independent Public Health Care Centre	income: 286.8 costs: 280.6
Regional Complex Hospital in Kielce	312.9
Świętokrzyskie Psychiatry Centre in Morawica	56.2
Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź	income: 410.8

Source: own preparation on the basis of the research. The table contains data obtained from the respondents. Some of them provided accounting information concerning income and costs. Some respondents gave only single amounts of the entity's budget.

Question 2. What are your expenses for ensuring information security in 2017 (consider equipment, software, training services, other services, other expenses)? Eight of the surveyed entities declared that in 2017 they had allocated funds to information security. Table 4 presents the amounts listed by category. Considering that "Pomeranian Hospitals" is a company comprised of 4 specialized hospitals, in 2017 they spent the largest amount on ensuring information security (even if the amount is divided into four units). The smallest amount was allocated by "Stanisław Rybicki Regional Hospital in Skierniewice" – almost 15 thousand zlotys. It should be noted that four entities did not indicate any amounts.

Question 3. Is the effectiveness of expenditure on information security measured? If so, please specify what method is used?

Of the ten respondents, the effectiveness of expenditure on information security is measured only by one. The entity does not use any specific method.

Question 4. In 2017, did the entity receive co-financing from external institutions, including the founding body, for tasks related to ensuring information security? If yes, please provide the name of the institution and the amount of funding in zlotys.

None of the entities had received subsidies from superior institutions for tasks related to ensuring information security in 2017. Only one declared that the hospital was a partner of the Regional Operational Program for the Świętokrzyskie voivodeship for the years 2017-2020 carried out by the Marshal's Office. The project aims to acquire the funds necessary for the proper electronic work of medical documentation. For the hospital, a total of over 4 million zlotys is planned.

Table 4. Expenses for ensuring information security in the surveyed entities in 2017

Entity	**Expenses for ensuring information security (zlotys)**	**Including, in particular:**				
		equipment (zlotys)	software (zlotys)	training services (zlotys)	other services (zlotys)	other expenses (zlotys)
Pomeranian Hospitals	2,060,410.00	1,355,593.00	547,000.00	1,700.00	36,285.00	119,832.00
Stanisław Rybicki Regional Hospital in Skierniewice	14,834.80	0.00	13,234.80	1,600.00	0.00	0.00
Regional Centre for Occupational Medicine Prevention and Medicine in Łódź	62,840.46	43,855.40	0.00	1,628.37	9,101.69	8,255.00
Dr Biegański Regional Specialist Hospital in Łódź	42,897.62	31,440.12	0.00	6,457.50	0.00	5,000.00 (locks for wardrobes, wardrobes)
Regional Complex Hospital in Kielce	124,592.00	39,317.00 (16 computer sets)	33,210.00 (ESET software) 52 065,00 (Fortigate upgrade)			
Świętokrzyskie Psychiatry Centre in Morawica	66,420.00				66,420.00	
Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź	99,216.63	98,903.63		313.00		
Maria Skłodowska-Curie Regional Specialist Hospital in Zgierz	26,600.00				26,600.00 (ISO/IEC 27001 implementation)	
Total for all entities (zlotys):	2,497,811.51	1,569,109.15	645,509.80	11,698.87	138,406.69	133,087.00
Total for all entities (%)	100	62.8	25.8	0.5	5.5	5.3

Source: own preparation on the basis of the research. The amounts of "Expenses for ensuring information security" are sums of values given in the following columns. The amounts of "Total for all entities (zlotys)" are sums of values given in the above rows. The values in the last row are the values of "Total for all entities (zlotys)" expressed as a percentage.

Question 5. Please enter the amount of expenses for implementing the changes resulting from the implementation of the GDPR.

Two of the entities indicated amounts: 33,110.00 zlotys and 24,000.00 zlotys. One of the entities claimed that changes resulting from the GDPR were implemented by the Information Security Administrators. The company did not incur additional costs (other than employees' salaries) related to this. The task was within the scope of the Administrator's responsibilities. Another hospital indicated that there was no possibility of separate expenses in 2017. Other units did not indicate any amounts.

Question 6. How many people are employed per FTE (as at the end of 2017)? and Question 7. How many patients are treated annually (as at the end of 2017)?

The last questions concerned the number of employees and the number of patients. The results are presented in Table 5.

Table 5. Number of employed people and number of patients in the surveyed entities in 2017

Entity	Number of Full-time equivalents (FTEs)	Number of patients
Pomeranian Hospitals	2625.13	approx. 341,000
Specialist Psychiatric Health Care Team in Łódź	458.55	141,488
Stanisław Rybicki Regional Hospital in Skierniewice	594.61	23,848 (hospitalizations) and 71,391 (outpatient treatment)
Regional Centre for Occupational Medicine Prevention and Medicine in Łódź	190.93	185,523 (outpatient treatment) and 19,943 (rehabilitation and dentistry)
Maria Skłodowska-Curie Regional Specialist Hospital in Zgierz	857.34	150,000
Dr Biegański Regional Specialist Hospital in Łódź	757.54	17,941 (hospitalizations) and 79,152 (outpatient treatment)
Świętokrzyskie Oncology Centre, Independent Public Health Care Centre	1554	24,856 (hospitalizations) 242,469 (outpatient treatment)
Regional Complex Hospital in Kielce	2119.18	65,490 (hospitalizations) and around 100,000 (outpatient treatment)
Świętokrzyskie Psychiatry Centre in Morawica	898.17	10,562
Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź	2218.57	69,880 (hospitalizations) 331 (rehabilitation) and 299,749 (outpatient treatment)

Source: own preparation on the basis of the research.

There are three entities with large numbers of FTEs: “Pomeranian Hospitals”, “Copernicus Regional Multispecialist Oncology and Traumatology Centre in Łódź” and “Regional Complex Hospital in Kielce”. This table shows how many people from the medical staff should be trained in the field of information security. In the context of this question, the amounts indicated for training services (Question 2) are too low in relation to the number of employees.

It also shows the number of people whose personal data (including sensitive data) go to IT operating systems in healthcare entities and which might be exposed in a data breach.

After analysing the results, it can be noticed that the methods of information security management (in terms of the surveyed aspects) are different in each of the surveyed entities.

The main concern is when there is only one person to ensure information security (there were two cases among the surveyed entities). It is impossible for a single individual to carry out their duties 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 inappropriately classifying incidents or interpreting the definition of incident differently.

It is also necessary to devote adequate resources from the budgets to manage information security.

All the respondents declared that the available financial resources are not enough. These resources should be allocated not only for software, hardware, and training but also to support IT administrators. In the respondents’ opinion, the management staff usually have a problem understanding that teams have too few members and the scope of duties is increasing (monitoring responsibilities are increasing, the administrator's work is needed non-stop, and often there is a need for an immediate reaction to an incident). In order to ensure proper protection, it is necessary to allocate financial resources to increase the information security teams.

The lack of efficient information security management in medical entities may impact future incidents.

The results of the research are consistent with the results of the 2018 HIMSS Cybersecurity Survey (HIMSS, 2018) in which the biggest barriers to the management of cybersecurity incidents is the lack of appropriate cybersecurity personnel (52.4%) and lack of financial resources (46.6%).

The results of the last part of the research confirmed that the entities allocated small amounts of their budgets to expenses related to information security; what is more, the effectiveness of these expenses is not measured. Analysis of the expenses on information security for all surveyed entities confirmed that most funds are spent on the purchase of hardware and software.

In the surveyed period, none of the entities received co-financing from external institutions in the field of information security. Only one unit declared that it would receive such funding in the future.

Some problems also occurred in determining the expenses for preparing an organization to implement changes resulting from the GDPR. It should be highlighted that the new regulations came into force on 25 May 2018, and some units might have included such expenses in their budget for 2018. However, it seems that the implementation of such a project in less than half a year would not have ended in the timely implementation of all changes. The analysis of the implementation process of the GDPR is the subject of further research by the authors. Admittedly, the situation is very serious, and there were cases of administrative fines: for example, the National Data Protection Commission imposed a fine of 400,000 euro at the Barreiro Montijo Hospital in Portugal (Irwin, 2018).

As demonstrated in the article, units performing medical activities are exposed to a number of attacks by cybercriminals. The results of the study confirmed how much personal data, including sensitive data, are processed in the surveyed units.

On the other hand, it is important to ensure an adequate level of security to warrant the continued running of these units. Hospitals cannot afford a few days' shutdown, as happened in British hospitals in 2017 due to a massive ransomware attack (Brandom, 2017).

Conclusions

As a result of the research, it could be concluded that information security management in entities performing medical activities is carried out in an inadequate way. Most of the surveyed entities do not allocate any financial resources to ensure information security, which can cause serious consequences, particularly in relation to administrative fines specified in GDPR. Entities performing medical activities should allocate more financial resources to ensure an adequate level of information security; however, this is connected with the necessity of local government administration co-financing these units. In the context of further research, a survey in entities performing medical activities from the other voivodeships in Poland, as well as other countries, is planned.

References

Appari, A., Johnson, M.E. (2010). Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management*, 6(4): 279-314.

Brandom, R. (2017). UK hospitals hit with massive ransomware attack. Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

Chen, Y.P., Hsieh, S.H., Cheng, P.H., Chien, T.N., Chen, H.S., Luh, J.J., Lai, J.S., Lai, F.L., Chen, S.J. (2010). An Agile Enterprise Regulation Architecture for Health Information Security Management. *Telemedicine Journal and E-health*, 16(7): 807-817.

Constitution of RP (1997). Constitution of the Republic of Poland of 2nd April, 1997. Retrieved from http://www.sejm.gov.pl/prawo/konst/polski/ kon1.htm.

Davis, J. (2018a). Nearly 280,000 Medicaid patient records breached in Oklahoma hack. Retrieved from https://www.healthcareitnews.com/news/nearly-280000-medicaid-patient-records-breached-oklahoma-hack.

Davis, J. (2018b). Medical data of 33,000 BJC HealthCare patients exposed online for 8 months. Retrieved from https://www.healthcareitnews.com/news/medical-data-33000-bjc-healthcare-patients-exposed-online-8-months.

Davis, J. (2018c). Ransomware attack on fetal diagnostic lab breaches 40,800 patient records. Retrieved from https://www.healthcareitnews.com/news/ransomware-attack-fetal-diagnostic-lab-breaches-40800-patient-records.

EU (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 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 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 from https://www.beyondtrust.com/blog/fallout-mongodb-breaches/.

Haertle, A. (2017). Wyciek danych wrażliwych 50 tysięcy pacjentów polskiego szpitala. [A leak of the sensitive data of 50,000 patients in a Polish hospital]. Retrieved from https://zaufanatrzeciastrona.pl/post/wyciek-danych-wrazliwych-50-tysiecy-pacjentow-polskiego-szpitala/.

Herjavec Group (2019). The 2019 Healthcare Cybersecurity Report. Retrieved from https://www.herjavecgroup.com/2019-healthcare-cybersecurity-report/.

HIMSS (2018). 2018 HIMSS Cybersecurity Survey. Retrieved from https://www.himss.org/sites/hde/files/d7/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*, 126: 64-75.

International Organization for Standardization (2016). ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002, Geneva, ISO.

Irwin, L. (2018). Portuguese hospital appeals GDPR fine' IT Governance. Retrieved from https://www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine.

Lisiak-Felicka, D., Nowak, P. (2018). RODO w podmiotach wykonujących działalność leczniczą. Wybrane zagadnienia. [GDPR in entities performing therapeutic activity. Selected aspects], *Przedsiębiorczość i Zarządzanie* XIX(5), Part 1: 57-67.

Lisiak-Felicka, D., Nowak, P., Szmit, M. (2018). Selected aspects of information security management in entities performing medical activity. *Economic and Social Development 34thInternational Scientific Conference on Economic and Social Development – XVIII International Social Congress* (ISC-2018) Book of Proceedings: 51-60.

Lisiak-Felicka, D., Zajdel-Całkowska, J., Zajdel, R. (2017). Wybrane aspekty zarządzania bezpieczeństwem informacji w podmiotach prowadzących działalność leczniczą. [Selected aspects of information security management in entities performing therapeutic activity], *Przedsiębiorczość i Zarządzanie*, XVIII(4), Part 2: 167-180.

Maj, M. (2017). Dane setek pacjentów na serwerze zewnętrznej firmy obsługującej szpitale. [Data leak of hundreds of patients on the server of an external company serving hospitals]. Retrieved 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): 47-50.

Ministry of Health (2018). Statistical Bulletin of the Ministry of Health. Retrieved from https://www.csioz.gov.pl/fileadmin/user_upload/Biuletyny_informacyjny/biuletyn_2018_5c3deab703e35.pdf.

Morse, S. (2018). CMS responds to data breach affecting 75,000 in federal ACA portal. Retrieved from https://www.healthcarefinancenews.com/news/cms-responds-data-breach-affecting-75000-federal-aca-portal.

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*, 113: 653-658.

Ponemon Institute (2018). 2018 Cost of a Data Breach Study. Global Overview, Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. Retrieved from https://www.ibm.com/downloads/cas/AEJYBPWA.

Regional Information Service (2018). Jednostki podległe. [Subordinate units]. Retrieved from http://www.zdrowie.lodzkie.pl/zadania-departamentu/jednostki-podlegle.

Sánchez-Henarejos, A., Fernández-Alemán, J.L., Toval A., Hernández-Hernández I., Sánchez-García A.B., Carrillo de Gea, J.M. (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): 214-22.

UoDL (2011). Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej. [Act of 15 April 2011 on Medical Activity]. (Dz.U.2011 Nr 112 poz. 654).

UoSG (1998). Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym. [Act of 8 March 1990 on Municipal Government]. (Dz.U. 1990 Nr 16 poz. 95).

UoSOZ (2004). Ustawa z dnia 27 lipca 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. [Act of 27 July 2004 about health care benefits financed from public funds]. (Dz.U.2004 Nr 210 poz. 2135).

UoSP (1998). Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym. [Act of 5 June 1998 on poviat local government]. (Dz.U. 1998 Nr 91 poz. 578).

UoSW (1998). Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa. [Act of 5 June 1998 on the voivodeship local government]. (Dz.U. 1998 Nr 91 poz. 576).

Voight, P., von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer International Publishing AG.

Woo-Sung, P., Sun-Won, S., Seung-Sik, S., Mee--Jeong, L., Shin-Hyo, K., Eun-Mi, Ch., Ji-Eon, B., Yea-Eun, K., Ok-Nam, K. (2010). Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds. Healthcare Informatics Research, 16(2): 89-99.

Zammani M., Razali R. (2016). Information Security Management Success Factors, *Advanced Science Letters,* 22(8): 1924-1929.

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*, 9: 75-85.