Pomeranian J Life Sci 2021;67(2):48-54 doi: 10.21164/pomjlifesci.700

An assessment of knowledge on the protection of personal data among nursing staff*

Angelika Lewandowska[1, A] ✉, Paulina Mariola Stróżyk[2, B], Magdalena Kabała[3, C], Dorota Kozieł[1, D]

[1] Jan Kochanowski University in Kielce, Collegium Medicum, IX Wieków Kielc 19, 25-317 Kielce, Poland
[2] Jan Kochanowski University in Kielce, Collegium Medicum, Provincial Specialist Hospital of St. Rafał in Czerwona Góra, Czerwona Góra 10, 26-060 Chęciny, Poland
[3] Jan Kochanowski University in Kielce, Collegium Medicum, Holycross Cancer Center in Kielce, Artwińskiego 3, 25-734 Kielce, Poland

[A] ORCID: 0000-0003-2830-798X; [B] ORCID: 0000-0001-6030-6659; [C] ORCID: 0000-0002-1671-496X; [D] ORCID: 0000-0001-8114-1814

✉ lewandowska.a.m@wp.pl

ABSTRACT

Introduction: Numerous legal acts are in place to protect the personal data of patients. The Act on the Protection of Personal Data contains basic information on the principles of data processing, as well as specifying what criminal sanctions are in place for non-compliance.

The aim of the study was to assess the level of knowledge about personal data protection among nursing staff working in the Świętokrzyskie Province. Additionally, an analysis of the subjective assessment of whether there is a need for training in the field of personal data of the above-mentioned professional group was performed.

Materials and methods: The study was conducted among 141 male and female nurses working in the Świętokrzyskie Province. The study group consisted of 109 people working in the hospital and 32 people working in primary health care. The average age of respondents was 41.3 years. The study used the diagnostic survey method. A tailored questionnaire was used to assess knowledge about the protection of personal data. The obtained results were statistically developed using Excel. The present study used the χ^2 test and statistical significance was assumed at the level of $p < 0.05$.

Results: Among of respondents 89% selected paper and electronics as the leading methods of storing data. A very small number of respondents, namely about 4% of the surveyed people, have passed patient information to a third party. Among of people 81% are aware of the criminal liability for violating the provisions on the protection of personal data. Less than half of the respondents (38%) knew the correct length of time that medical records can be stored – 20 years. No relationship was found between the type of workplace and demand for training, and the type of workplace and the subjective assessment of the level of knowledge of the respondents in the field of personal data protection.

Conclusions: Nursing staff working in primary health care show a greater need for training on the General Data Protection Regulations (GDPR) than nursing staff working in hospitals. There is no statistically significant difference between the workplace of nursing staff and the demand for training. The subjective assessment of knowledge of the respondents in the field of personal data protection in the case of hospital nurses is low, and in the case of primary health care employees is average.

Keywords: personal data protection; sensitive data; nursing staff; GDPR.

INTRODUCTION

Only a dozen or so years ago, medical facilities largely stored documents in paper form, and filing cabinets with patient records filled archives. Nowadays, new technologies allow for the implementation of information technology (IT) systems in which patients' personal data can be entered. However, the processing of this data must be properly secured. The General Data Protection Regulation (GDPR) applies to both business and healthcare environments. The above regulations contain a set of provisions that inform entrepreneurs and consumers about their rights and obligations in the field of information processing and storage [1, 2, 3, 4].

In 2012, a draft GDPR was presented and the final form was approved in 2016. In all European Union countries, including Poland, the GDPR came into force on May 25, 2018. The introduction of a new personal data security policy grants numerous rights and imposes obligations on both entrepreneurs and consumers. The most important obligations that enterprises must fulfill include: the establishment of a Data Protection Officer (DPO) where data processing is at the core of their activities, reporting data leaks within 72 h of the moment violations are detected, and documenting how personal data is processed with regard to the type of data, the purpose of processing and the information of the person responsible for it. In turn, consumers under the new provisions may exercise their rights such as, among others: the right to access their data (the consumer may request detailed information about the data collected and processed about them), the right to transfer data (the consumer has the right to request the export of personal data and transfer them to another company), the right

* This work was supported under the program of the Minister of Science and Higher Education named "Regional Initiative of Excellence" in 2019–2022, project number: 024/RID/2018/19, financing amount: 11,999,000.00 PLN.

to correct personal data (the consumer will be free to change the information collected by the company), and the right to be forgotten (the consumer will be able to force the removal of the collected information about themselves) [4, 5, 6, 7, 8].

The first attempts to implement electronic medical records (EMR) in Poland were scheduled for August 2014. Unfortunately, due to the maladjustment of IT systems, this deadline was repeatedly shifted. Ultimately, the obligation to implement EMR by medical entities was applied on 1 January 2019. Due to the fact that work in medical facilities is mainly conducted on special computer systems, there is a need to conduct training for doctors, nurses and other medical staff in the use of such a system and how to securely store information about patients. Year-on-year, the level of protection against cyberattacks increases, however, increasingly sophisticated cyberattacks are also emerging [1, 2, 3]. In the case of the GDPR, there are certain technical requirements which, when fulfilled, have an impact on increasing the security of stored data. Care should be taken of elements such as: the protection of company computers and mobile devices (legal and up-to-date software, the use of secure passwords, antivirus programs), data leakage prevention and data encryption (professional software, NAS servers, encrypted portable memory drives, cloud data storage), monitoring of company resources and supervision over permissions, current documentation and secure data transfer during equipment replacement. It is essential to remember to permanently delete data saved on devices and media that are to be destroyed. The outsourcing of data storage by medical institutions is gaining popularity. The change in regulations forces the above entities to increase the level of security for stored data [4, 9].

Therefore, attention should be paid to the proper use of new information technologies that allow for an increase in the potential and efficiency of the institution. This translates into reducing the cost of the facility and increasing the level of the quality of care [1].

In order for all aspects of personal data security, processing and storage to be met, an efficient IT system with appropriate functions is needed. Such a system should be based on key elements such as:

— Hospital Information System (HIS), whose main job is to run the patient database; it is also responsible for archiving or sending information to other medical facilities,

— Picture Archiving and Communication System (PACS), which is responsible for archiving and allows you to capture images from diagnostic apparatus,

— Radiology Information System (RIS), used in the field of radiology, combines elements of the HIS and PACS,

— Laboratory Information System (LIS), which deals with the faster collection of samples, storage, coding and labeling in healthcare facilities,

— Pharmacy Information System (PIS), which plays a role in the demand, management and organization of drugs.

Access to IT systems for medical workers in institutions is available 24 h/day, 7 days a week. The main assumption is to enter patient data once [10, 11, 12, 13, 14, 15, 16].

The introduction of the GDPR caused various questions and doubts regarding the application of the new provisions by medical staff. When registering a patient, the risk of disclosing information to bystanders, especially health data, should be minimized and the activities must not interfere with the provision of healthcare services. In order to improve registration, a separate, designated place should be available where the patient themselves, or possibly their guardian or a family member / close person, can go through the registration process. The key points regarding the protection of personal data are: the meticulous acquisition of information, skillful processing and securing of data, only obtaining necessary data, as well as finding a suitable place so that the patient feels safe and can be listened to by medical personnel [17, 18, 19]. However, the provisions of the GDPR are secondary to the obligation to save human health and life.

The aim of the study was to assess the level of knowledge about personal data protection among nursing staff working in the Świętokrzyskie Province. Additionally, an analysis of the subjective assessment of the need for training in the field of personal data of the above-mentioned professional group was performed.

MATERIALS AND METHODS

The study was conducted in June 2019. The study group consisted of 141 male and female nurses working in the Świętokrzyskie Province. The study group consisted of 109 people working in the hospital and 32 people working in primary health care. The age of the respondents ranged 22–68 years. The average age of the respondents was 41.3 years. The study was carried out using the diagnostic survey method. A unique questionnaire, comprising 22 questions, was used. The survey was divided into 2 parts. The 1st contained a record and the 2nd part consisted of questions regarding the protection of personal data. An analysis of the demand for training and a subjective analysis of the level of knowledge of the respondents in the field of personal data security, depending on the workplace, was performed. Completing the questionnaires was fully anonymous and voluntary. The obtained results were statistically processed using Excel. The present study used the χ^2 test, statistical significance was assumed at $p < 0.05$.

RESULTS

The study group included 109 (77%) people working in a hospital and 32 (23%) people working in primary health care. The age of the respondents ranged 22–68 years. The mean age of the respondents was 41.3 years, the median was 41 years, and the standard deviation was 10.7 years. Among 141 respondents, the biggest group were people between 31–50 years of age (60% of respondents). Among the nursing staff, 123 (87%) were women and 18 (13%) were men (Fig. 1, Tab. 1).

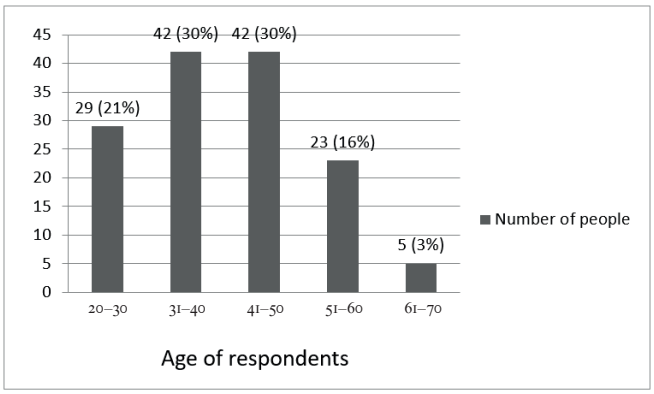

FIGURE 1. Age range of nursing staff

TABLE 1. Characteristics of the studied group by sex and workplace

	Sex		Workplace	
	female	male	hospital	primary health care
n	123	18	109	32
%	87	13	77	23

The vast majority of respondents, 88% to be exact, said that they know of GDPR and are able to expand the abbreviation while 12% of respondents claimed to have no knowledge of the regulation. When asked if they know what sensitive personal data are, most of the respondents, 78 people (55%), answered that they did not know. Only 63 (45%) of the respondents indicated that they know what sensitive data are; 77 (55%) people were able to explain the term "ordinary personal data". Only 36 (26%) of the surveyed people knew what the rights of new patients are, as implemented by the GDPR (Fig. 2).

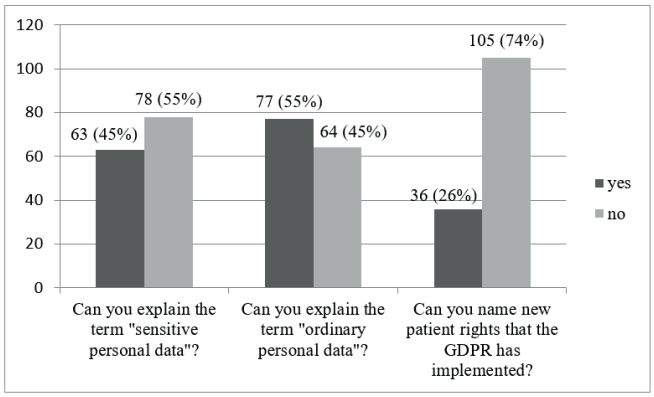

FIGURE 2. Nursing staff's knowledge about personal data

Among respondents, 106 (75%) said they had a DPO (formerly the Information Security Administrator) at their workplace, while 35 (25%) of the employees did not know that they have a DPO. One hundred and nine people (77%) indicated that they were familiar with the Information Security Policy, however, 32 (23%) of the respondents were not aware about them in their workplace. According to the data analysis, 98 (70%) respondents were familiar with the Information System Management Manual (Fig. 3).

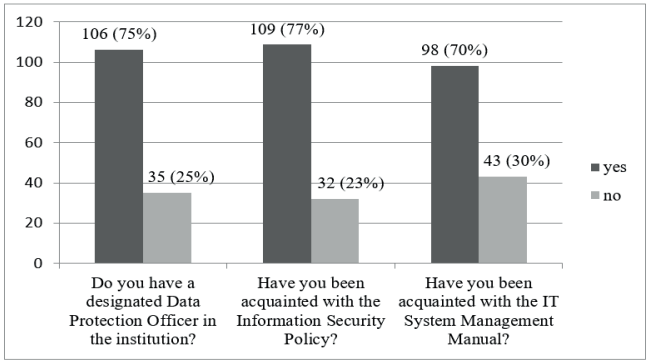

FIGURE 3. Nursing staff's knowledge in the field of online security

Nearly 89% of respondents working in various medical units store patient data in 2 forms: paper and electronic. Only 7% of respondents base their work on medical documentation purely in paper form, and 4% purely in electronic form. When presenting the results of the respondents' knowledge in the field of personal data protection, 103 (73%) of the respondents indicated that they are aware of how to secure patients' personal data in paper form, while 38 (27%) were not informed about the correct handling of the above-mentioned data. Regarding knowledge about how to secure patients personal data on electronic devices, as many as 90 (64%) of the respondents stated that they know how to do this, while 51 (36%) people indicated that they have no knowledge in this regard (Fig. 4).

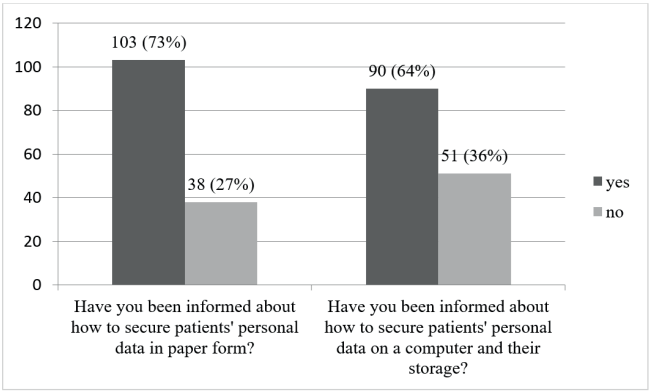

FIGURE 4. Number of nursing staff informed about the principles of personal data protection

The respondents were asked about the scope of data that is processed in the computer system. From the selected categories, 22% of respondents indicated that the patient's first and last name, date of birth, parents' names, home address, PESEL number, identity card number and medical history were collected. Among of respondents 23% do not know the correct storage time for medical records. Two people indicated that medical records should be kept for 1 year or 3 years, 12% of respondents said that medical records should be kept for 5 years, 13% indicated a period of 10 years and 2% specified 15 years. The correct answer – 20 years – was indicated by 38% of respondents. A few people (4–7%) said that medical records were kept for 25–30 years, respectively. Nursing staff were

also asked about giving patient information to third parties. Only 4% of the respondents said they had done this, and analogously, 96% had not. In the question regarding the awareness of criminal liability for violations of data protection, 81% of respondents gave an affirmative answer, while 19% were not aware of criminal liability.

Another aspect of the research was an assessment of data protection knowledge among nursing staff depending on sex and workplace. Male nurses showed a lower level of knowledge concerning, inter alia, the method of securing patients' personal data in paper form and knowledge of the term "sensitive personal data" compared to female nurses (Tab. 2).

TABLE 2. Assessment of the level of knowledge on personal data protection among nurses depending on sex

Feature	Division of the study group by sex			
	nurses		male nurses	
	n	%	n	%
Can you explain the term "sensitive personal data"?				
Yes	56	45.5	7	38.9
No	67	54.5	11	61.1
Can you explain the term "ordinary personal data"?				
Yes	67	54.5	10	55.5
No	56	45.5	8	44.5
Can you name new patient rights that the General Data Protection Regulation has implemented?				
Yes	33	26.8	3	16.7
No	90	73.2	15	83.3
Do you have a designated Data Protection Officer in the institution?				
Yes	93	75.6	13	72.2
No	30	24.4	5	27.8
Have you been acquainted with the Information Security Policy?				
Yes	96	78.0	13	72.2
No	27	22.0	5	27.8
Have you been acquainted with the IT System Management Manual?				
Yes	85	69.1	13	72.2
No	38	30.9	5	27.8
Have you been informed about how to secure patients' personal data in paper form?				
Yes	91	74.0	12	66.7
No	32	26.0	6	33.3
Have you been informed about how to secure and store patients' personal data on a computer?				
Yes	78	63.4	12	66.7
No	45	36.6	6	33.3

More nurses working in primary health care were aware of how to secure patients' personal data in paper form than on a computer. On the other hand, the knowledge of network safety rules was higher among people working in hospitals (Tab. 3).

TABLE 3. Assessment of the level of knowledge on personal data protection among nurses depending on the workplace

Feature	Division of the study group according to the workplace			
	hospital		primary health care	
	n	%	n	%
Can you explain the term "sensitive personal data"?				
Yes	52	47.7	11	34.4
No	57	52.3	21	65.6
Can you explain the term "ordinary personal data"?				
Yes	64	58.7	13	40.6
No	45	41.3	19	59.4
Can you name new patient rights that the General Data Protection Regulation has implemented?				
Yes	25	22.9	11	34.4
No	84	77.1	21	65.6
Do you have a designated Data Protection Officer in the institution?				
Yes	81	74.3	25	78.1
No	28	25.7	7	21.9
Have you been acquainted with the Information Security Policy?				
Yes	86	78.9	23	71.9
No	23	21.1	9	28.1
Have you been acquainted with the IT System Management Manual?				
Yes	79	72.5	19	59.4
No	30	27.5	13	40.6
Have you been informed about how to secure patients' personal data in paper form?				
Yes	78	71.6	25	78.1
No	31	28.4	7	21.9
Have you been informed about how to secure and store patients' personal data on a computer?				
Yes	69	63.3	21	65.6
No	40	36.7	11	34.4

When asked about the need to introduce training on the subject of GDPR, the vast majority of respondents – 132 (94%) – expressed that there is a need for training in medical facilities and only 9 (6.4%) respondents were against this. The last question in the survey allowed for an assessment of the level of knowledge of the respondents regarding the GDPR. The results were as follows: 63 (44.7%) respondents indicated a low level of knowledge about GDPR, 70 (49.6%) people indicated an average level, and only 8 (5.7%) people rated their level of knowledge as high (Fig. 5, 6).

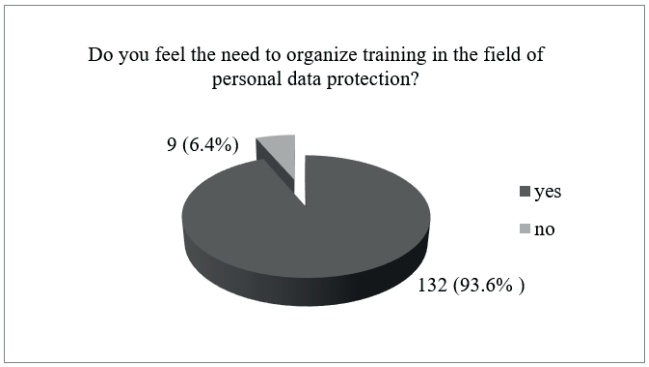

FIGURE 5. Opinion of respondents on the need to organize training in the field of personal data protection

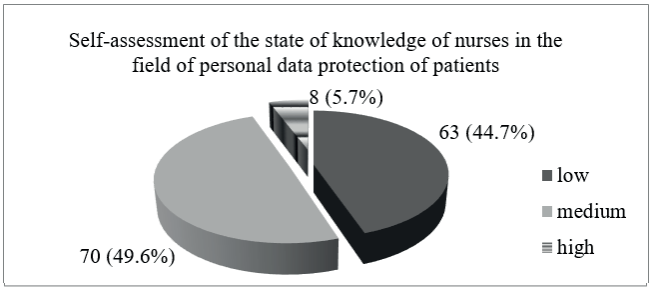

FIGURE 6. Subjective assessment of the level of knowledge of respondents in terms of General Data Protection Regulation

TABLE 4. The relationship between the workplace and the need for training in personal data protection

		Workplace				Total	
		hospital		primary health care			
		n	%	n	%	n	%
Demand for training	yes	102	72.3	30	21.3	132	93.6
	no	7	5.0	2	1.4	9	6.4
Total		109	77.3	32	22.7	141	100

χ^2 = 0.97208; df = 1; p = 0.324

TABLE 5. The relationship between the workplace and the subjective assessment of the level of knowledge of the respondents in the field of personal data protection

		Workplace				Total	
		hospital		primary health care			
		n	%	n	%	n	%
Subjective assessment of the level of knowledge of the respondents	low	53	37.6	10	7.1	63	44.7
	medium	49	34.7	21	14.9	70	49.6
	high	7	5.0	1	0.7	8	5.7
Total		109	77.3	32	22.7	141	100

χ^2 = 0.117994; df = 2; p = 0.943

The following statistical analysis shows that there is no statistically significant correlation between the workplace and the demand for training (p = 0.324), and the workplace and the subjective assessment of the level of knowledge of the respondents in the field of personal data protection (p = 0.943). A greater demand for training was observed among nursing staff working in primary health care. Despite the smaller group of people working in primary health care in the study, as many as 30 out of 32 people expressed their willingness to undergo training. In the case of a subjective analysis of the level of knowledge of the respondents in the field of personal data protection, the majority of hospital employees assessed their level of knowledge as low, while an average level of knowledge was dominant among primary health care employees (Tab. 4, 5).

DISCUSSION

In a report published by Deloitte in April 2011, it was estimated that 33% of Polish medical institutions did not use IT systems. In Europe, this number is 19% [12, 20]. The authors' research revealed that only 7% of respondents claim to only store patient data in a paper form.

According to a report published by the Supreme Audit Office, hospitals stored medical information about patients without properly securing it, for example, by not locking cabinets with a key or by leaving patient documentation on their desks [21]. A similar situation was found in primary health care facilities and non-public medical entities. It was reported that over half of them complied with the set requirements [22]. It is worth mentioning that in the report on foreign hospitals, in order for paper documentation to be secured, they should also be stored in rooms accessed by a special magnetic card, where access is limited [23]. Our research showed that 77% of respondents were familiar with the Information Security Policy. It seems that in order to prevent errors in processing information, the nursing staff should be properly trained.

In the Supreme Audit Office report published in April 2013, 944 units took part in the study, of which only 421 institutions were compliant with all regulations. Among of facilities 31% did not have IT systems and were unable to enter patient data electronically. About 20% of the facilities did not have access to the HIS, 40% to LIS and as much as 67% to RIS. The PIS operated in 77% of facilities. In these institutions, 96% of nursing staff surveyed use IT systems for patient data [12, 24]. In the authors' research, 93% of respondent use information systems to process patient data.

In hospitals, problems that occur at the level of anti-virus security are the lack of anti-virus software updates, as well as the sharing of passwords and login IDs between medical staff [21]. Foreign hospitals struggled with similar irregularities. An additional security threat mentioned in the report was the setting of a specific amount of time in the system to enter information about the patient [23]. According to the results of our research, 36% of respondents admitted that they do not have any knowledge in the field of computer hardware security at work. This ignorance implies a risk of disclosing personal data to unauthorized persons. The analyzed data from the Supreme

Audit Office from 2015 shows that the biggest issue in care and treatment institutions was the securing of patients' medical records (almost 63%). In inpatient treatment, the safety and protection of personal data amounted to almost 53%, while in outpatient treatment – almost 45% [22].

Analyzing the data published by Jacek et al., it can be seen that about 77% of medical personnel confirm that there are appropriate regulations regarding the dissemination and processing of personal information in their databases. Managing the proper archiving of medical documents is primarily the responsibility of the managers of the institution and the medical personnel (60%) [5]. In our research, 75% of respondents confirmed that they have a DPO at their workplace. People should strive for the broadest possible information about the activities of the DPO.

The report from the Supreme Audit Office noted that information about patients in hospitals was made available to third parties against the patient's will. It was noted that some irregularities occurred in hospitals – non-medical staff at the facilities had access to medical histories and the results of medical examinations [21]. According to our research, 4% of respondents revealed information about patients to third parties.

The majority of respondents believe that patient data should be stored for 10 years (37%). Other respondents reported that the correct time for keeping documents is 5 years (approx. 24%), 15 years (20%) and 20 years (19%). Due to care for the security of storing archived data, the respondents believe that the type of information contained in the files is of significant importance related to the time of their collection (72%).

In primary health care facilities and foreign hospitals, it was noted that medical documentation was often incomplete or illegible and that there was no information on the patient's medical history and procedures performed. As well as this, the page numbering in the patient files was not correct. Such negligence may lead to a medical misdiagnosis [22, 23]. In the authors' own research, the respondents answered that the first name, surname and place of residence constituted personal data (98%), as did the PESEL number (94%). A minority (30%) of the respondents claimed that the telephone number and place of employment are not personal data.

According to a study by Szymczyk and Horoch, approx. 94% of respondents (medical staff and medical registrars) were familiar with the published rules of using a computerized patient database, while 53% knew that instructions on how to handle electronic personal data are found in the regulations. It was noted that there were problems with the implementation and use of e-documentation in the facility. There were many requests for help to the IT department on how to handle electronic records – 40% from doctors and 60% from nurses [25]. According to our research, 70% of respondents were familiar with the IT System Management Manual. When asked about the length of the training, 38% of respondents said that it was not enough to get acquainted with the skills needed for entering personal data.

Szymczyk and Horoch reports that the procedure of converting paper medical documentation to electronic form was of great importance to nursing staff and registrars, as it significantly improved the formalities related to patient registration by up to 80%, and the transparency of information and medical history about the person being treated (70%). Additional aspects include minimal consumption of printer consumables (70%), security of patient's personal data (92%) and easy access to information (83%), which is associated with better efficiency [26]. Our research has shown that almost 89% of the medical personnel in the surveyed facilities rely on both paper and electronic documentation. The respondents are able to secure information about patients in a correct manner – paper form 73% and electronic form 64%.

The research results provided by Kilańska show that training on the use of e-documentation is necessary for properly functioning medical facilities (83%) [27]. In our study, 94% of respondents indicated the need to conduct the above training in medical facilities and only 6% of respondents were against this.

The protection of patients' personal data is one of the many aspects often overlooked in the nursing profession. Reasons for this include, among others: insufficient knowledge in this area, uncertainty about the correct application of legal provisions and an overwhelming number of other basic obligations that leave little time for duties of a non-medical nature. This is why it is important to implement education for nurses with a wide scope of information regarding the protection of patients' personal data.

CONCLUSIONS

Nursing staff working in primary health care show a greater need for training on the GDPR than nursing staff working in a hospital. There is no statistically significant difference between the workplace of nursing staff and the demand for training.

The subjective assessment of the knowledge of the respondents in the field of personal data protection in the case of hospital nurses is low, and in the case of primary health care employees is average.

REFERENCES

1. Nyczaj K, Piecuch P. Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej. Warszawa: Wydawnictwo Wiedza i Profilaktyka; 2014.
2. Hołyst B, Pomykała J. Cyberprzestępczość, ochrona informacji i kryptologia. Prokuratura i Prawo 2011;1:5-34.
3. Ayala L. Cybersecurity for hospitals and healthcare facilities. A guide to detection and prevention. Virginia: Apress; 2016.
4. Ignar M. Co to jest RODO? Wszystko co musisz wiedzieć. 2018. https://www.komputronik.pl/informacje/co-to-jest-rodo-wszystko-co-musisz-wiedziec/ (8.04.2019).
5. Jacek A, Szwed K, Ożóg K, Porada S. Aspekty ochrony danych osobowych pacjentów w świetle obowiązujących regulacji prawnych w Polsce oraz Unii Europejskiej. Hygeia Public Health 2013;48(1):46-50.
6. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

7. Stępniewski R. RODO i nowe prawa osób, których dane dotyczą. 2018. https://www.politykabezpieczenstwa.pl/pl/a/rodo-i-nowe-prawa-osob-ktorych-dane-dotycza (5.02.2019).
8. Łokaj M. RODO w ochronie zdrowia – przewodnik po zmianach w zakresie ochrony danych osobowych. http://www.oipip.konin.pl/images/Alicja/rodoprzewodnik.pdf (5.02.2019).
9. Kamiński M. Powierzenie przetwarzania osobowych danych medycznych a perspektywy prowadzenie dokumentacji medycznej w postaci elektronicznej. CBKE e-Biuletyn 2007;3:1-14.
10. O'Connor S. What Are the Differences Between PACS, RIS, CIS, and DICOM? Advanced Data Systems Corporation; 2017. https://www.adsc.com/blog/what-are-the-differences-between-pacs-ris-cis-and-dicom (5.02.2019).
11. Keayes RG, Grenier L. Benefits of distributed HIS/RIS-PACS integration and a proposed architecture. J Digit Imaging 1997;10(3 Suppl 1):89-94.
12. Karlińska M. Informatyzacja opieki stacjonarnej w systemie ochrony zdrowia na przykładzie warszawskich szpitali publicznych. Studia Ekonomiczny w Katowicach 2014;199:99-106.
13. mediDOK. Archiwizacja badań diagnostycznych w Elektronicznej Dokumentacji Medycznej. Inżynier i Fizyk Medyczny 2018;7(3):161.
14. Babić RR, Milošević Z, Đinđić B, Stanković-Babić G. Radiology information system. Acta Medica Medianae 2012;51(4):39-46.
15. Aldosari B, Gadi HA, Alanazi A, Househ M. Surveying the influence of laboratory information system: an end-user perspective. Informatics in Medicine Unlocked 2017;9:200-9.
16. Isfahani SS, Raeisi AR, Ehteshami A, Janesari H, Feizi A, Mirzaeian R. The role of evaluation pharmacy information system in management of medication related complications. Acta Inform Med 2013;21(1):26-9.
17. Barta J, Fajgielski P, Markiewicz R. Ochrona Danych Osobowych. Warszawa: Wolters Kluwer Polska; 2011.
18. Jagielski M. Prawo do ochrony danych osobowych. Standardy europejskie. Warszawa: Oficyna a Wolters Kluwer Business; 2010.
19. Hoc S, Szewc T. Ochrona danych osobowych i informacji niejawnych. Warszawa: C.H. Beck; 2014.
20. European Commission. eHealth Benchmarking III. Report Deloitte & Ipsos Belgium 2011. https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ehealth_benchmarking_3_final_report.pdf (5.02.2019).
21. NIK. Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych. https://www.nik.gov.pl/plik/id,21467,vp,24109.pdf (5.02.2019).
22. NIK. Tworzenie i udostępnianie dokumentacji medycznej. https://www.nik.gov.pl/plik/id,10736,vp,13069.pdf (5.02.2019).
23. Data Protection Investigation in the Hospitals Sector. A report by the Special Investigations Unit of the Data Protection Commissioner's Office. Data Protection Commissioner; 2018. https://www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC%20-%20Hospitals%20Sector%20Overall%20Report%20_0.pdf (5.02.2019).
24. NIK. Informatyzacja szpitali. https://www.nik.gov.pl/plik/id,4849,vp,6462.pdf (5.02.2019).
25. Szymczyk DM, Horoch A. Implementacja elektronicznej dokumentacji medycznej. Część 3 – szkolenie personelu medycznego w zakresie technicznego i prawnego użytkowania danych sensytywnych. Med Og Nauki Zdr 2013;19(3):331-6.
26. Szymczyk DM, Horoch A. Implementacja elektronicznej dokumentacji medycznej. Część 1 – wpływ na efektywność pracy personelu medycznego. Med Og Nauk Zdr 2013;19(3):319-23.
27. Kilańska D. Elektroniczny rekord pacjenta w opinii pielęgniarek. Implikacje do dydaktyki – wykorzystanie narzędzi IT w nauczaniu klasyfikacji ICNP. Probl Pielęg 2017;25(2):69-76.