Family Medicine & Primary Care Review 2017; 19(3): 313–318 https://doi.org/10.5114/fmpcr.2017.69297

REVIEWS

© Copyright by Wydawnictwo Continuo

ISSN 1734-3402, eISSN 2449-8580

Current threats to medical data security in family doctors' practices

ROBERT SUSŁO[1, A, B, D–F], JAKUB TRNKA[2, A, D], JAROSŁAW DROBNIK[1, A, D]

[1] Department of Gerontology, Department of Public Health, Faculty of Health Sciences, Wroclaw Medical University, Poland
[2] Department of Forensic Medicine, Faculty of Medicine, Wroclaw Medical University, Poland

A – Study Design, **B** – Data Collection, **C** – Statistical Analysis, **D** – Data Interpretation, **E** – Manuscript Preparation, **F** – Literature Search, **G** – Funds Collection

Summary The recent massive worldwide WannaCry/WannnaDecryptor ransomware attack on medical information systems, beginning 12 May 2017, demonstrated that even a temporary loss of the ability to create, update, or access medical data is detrimental both to patients' medical safety and to medical professionals' ability to work. In Poland, medical documents exist in paper-based and electronic forms; complete migration to computer processing and storage of medical data has already been delayed for ten years. Securing paper-based medical documents is comparably easy; the most common problems are illegibility; loss of the file; and errors in filling out the document, such as failure to fill in the obligatory fields identifying the patient, the medical professional filling in the document, or the date and time of document creation; and faulty, missing, or irrelevant data pertaining to health state, diagnostics, or therapy. In contrast, making electronic medical files secure is no longer a single time-limited, well-defined event, but rather a dynamic, long-lasting process of balancing risks against protective measures in highly unpredictable environment. Any electronic medical record can be attacked in many different ways, including using social hacking, penetrating physical barriers, destroying computer hardware, or overcoming software-based security. Preventive measures include continuous education of staff; using IT specialists' help at setup and maintenance of computer systems; and repeatedly reassessing the threats that exist and the appropriateness of the measures taken to prevent the risks thus identified. The approaching coming into force of EU Regulation 2016/679 means increased medical data security requirements and elevated legal, formal, and financial risks resulting from infringement.

Key words: forensic medicine, medical records, family medicine, data security, electronic medical records, hacker attack.

Susło R, Trnka J, Drobnik J. Current threats to medical data security in family doctors' practices. *Fam Med Prim Care Rev* 2017; 19(3): 313–318, doi: https://doi.org/10.5114/fmpcr.2017.69297.

Incidence of threats to medical data

Primary care physicians rely heavily on the medical data they have collected, which they also need to share with numerous other institutions in order to ensure both the level of quality of the medical services they provide [1] and to cooperate effectively on the many tasks involved in the public health system [2]. In the recent massive worldwide hacking attack on information systems that began on May 12 2017, the ransomware known as WannaCry or WannnaDecryptor infected more than 1200 computers in Poland – a minute number compared to about 200,000 compromised systems all over the world. Ransomware – one of numerous types of malicious computer software or malware – uses strong encryption to prevent users from accessing their own data, requesting a ransom to be paid in exchange for decryption. In the last two years along, there has been a greater than fourfold increase in the number of such attacks, and the last quarter of 2016 had over 9,000,000 new recorded cases [3]. The WannaCry attack affected some medical information systems, revealing both their vulnerabilities and the disastrous effects of such attacks on medical services. One of the vivid examples is that of the National Health Service (NHS) in the United Kingdom, which suffered greatly, as 90% of the computers in use by the Service were running the outdated Windows XP operating system, which is vulnerable to this type of attack. As this version of the software is no longer supported by Microsoft, the vulnerability was not fixed, even though its existence has been known since March 2017 [4].

Since even temporary (not to mention permanent) loss of the ability to create, update, or access medical data can have extremely serious effects on both patients' medical condition and medical professionals' ability to do their jobs [5], it is crucial to define the main threats to medical data security in primary physicians' practices and point to the basic means of preventing them: analysis of the literature, journals and internet sources, including medical databases, points to several weak points that may be susceptible to harm from such threats.

Analog and electronic data

Two main types of medical documentation are found at present in Poland: paper-based and electronic records. In some other countries, medicine has already become almost paperless, but in Poland the phasing out of paper-based documents to process and store medical data has been postponed for more than 10 years. The causes are various: on one hand, the state has been unable to build the core computer infrastructure needed to serve as a common platform for medical data exchange; on the other hand, many overworked physicians still distrust computerized systems or consider them to be burdensome toys rather than useful tools. Polish medical society shows no great eagerness to migrate fully from paper files to electronic systems because the latter generate additional costs of setup and maintenance; the available software is often unergonomic, is inflexible, and cannot be adapted to users' emerging needs;

many medical professionals still have limited competence in data input through computer keyboards; and using an electronic system sometimes makes medical professionals feel they are losing control over their information and becoming dependent on IT specialists. Moreover, Polish law makes a medical professional fully responsible for securing the medical data – a field that is unlikely to be an area of particular expertise for doctors and nurses [6].

Securing paper documents

Although medical professional would often prefer not to have to become experts in either physical or computer security, the security procedures for paper documents tend to feel rather simple, as they can be considered as a well-defined sequence of events: a document is written on, stamped, and signed, and is then placed in a metal drawer equipped with a lock. The key is turned, removed from the keyhole, and placed safely into the physician's or nurse's pocket. Flood and fire alarms are installed, mouse traps are set, and the document can be considered secure. The document will also stay secure for the next 20–30 years demanded by law, even (or especially) if no one opens the drawer in the meantime. In case of any doubt about who wrote the document, when it was written, and whether it was tampered with, there are well-established methods and procedures used by experts in the analysis of handwritten and typed documents [7]. The problems associated with paper-based medical documents do not seem insurmountable and are most commonly limited to the proverbial illegibility of physicians' handwriting, stamps, and signature; the loss of a patient's file, or part of it, or mixing a particular file up with other files, making it difficult to locate when needed; mistakes in filling out forms, such as the lack of some important data like the identity of the patient or of the medical professional who filled in the document; the date and time the document was creation; or faulty, missing, or irrelevant data on health state, diagnostics, or therapy. Such problems can occur both in the case of internal medical documents, like a patient's file [8], and external medical documents, including prescriptions and hospital discharge notes [9]. Typically, the user of paper documents has a feeling of operating in a familiar and friendly environment, while being fully in control of the situation.

Secure electronic documents

With electronic records, things become counterintuitive. Digital data are not bound to a particular physical carrier, they can be easily copied, sent over longs distances, and lost or erased. Such data cannot be safely kept on a single storage device, as the ability to successfully retrieve the data from the device cannot be absolutely relied on, and becomes dangerously unlikely after only 3–5 years; data thus need to be stored concurrently in many places, backed up, archived, and transferred onto new storage devices on a regular basis. The greatest advantage of electronic data is that they are easy to search, combine, and merge, but to fully take advantage of these options, it is necessary to store the data on computer networks where the facts of data security mean that the odds of being compromised can at best be considered acceptably low, never reaching zero. This means that securing electronic medical files is not a single well-defined event limited in duration, but a dynamic and long-lasting process of balancing risks against protective measures in a highly unpredictable environment. Moreover, plain electronic data can be easily tampered with, leaving no obvious traces. It can also be created so as to mimic a document from a different author or a different time; such falsification is especially easy for anyone with administrative privileges on a computer system that does not have specially adjusted hardware and additional software supporting electronic signatures and timestamps. Possessing the data does not mean having access to the information any more, especially in light of no-longer supported data storage systems and file formats and encryption. Another major vulnerability is the dependency of information system on electrical power and internet access: any prolonged blackout or network failure makes all the data inaccessible [10]. The ease of operating on large blocks of data, especially text, creates new temptations for users. In particular, the reckless use of templates, copy–paste operations, and automatic data import from a wide variety of sources can lead to situations where there is an abundance of medical data accompanied by a scarcity of trustworthy medical information [6]. Needless to say, the careless approach towards maintaining and sharing medical data, which is still so common in electronic form, results in serious legal and other problems for medical professionals and their patients; these include a lack of reliable evidence resulting in subsequent poor quality, or even erroneous expert opinions [11] in case of accusations of medical error [12], criminal cases [13], domestic violence [14], sexual abuse [15], substance dependencies [16], and compensation for trauma-related health loss [17]. Another common problem is associated with the ease of transferring electronic data: a common dangerous activity that results from a false sense of security is sending unencrypted files containing sensitive medical data via e-mail or by fax, or simply discussing them over the phone [18]. Any medical professionals or patients who still feel they are in full control here are ignorant and, sooner or later, likely to be hopelessly lost.

Trying hard is not enough

Of course, the whole developed world now relies heavily on computer systems and electronic data. Most physicians and nurses in Poland also use them, either as the exclusive form of medical file storage or, more often, as a way of creating paper documents. Without computer support, it would be impossible today for a primary care physician to keep track with all the requirement of state and financial institutions, and especially to generate and deliver all the numerous reports of various kinds in a timely manner [19]. As no one is capable of abandoning all the electronic devices currently in use – including desktop and laptop computers, tablets, smartphones, and numerous strictly medical tools, like automated laboratory analysis devices – it is important to recognize threats and develop an individual risk-minimizing strategy.

An old and tested saying says people are the weakest link in any chain. Applying this to medical data security leads us to stress the role of ongoing education of all members of the primary physician's practice staff. Not only the physician and the nurse or midwife should be aware of threats and ways of managing them, but the technical and support staff should also be educated. This can be difficult as these people often come from an external contractor and staff rotation may be high. The education should include the accepted ways of solving common problems, as well as algorithms for use in nontypical emergencies. Typical scenarios include dividing the building into zones and restricting physical access to them to different categories of people, including permanent staff, patients, and external technical and maintenance support; reaction to disasters (floods, fires, and explosions) or intruders in the building; setting flow paths for paper documents of different types; a password policy for computer systems and the access permissions associated with it; a regular data backup and archiving policy, including a schedule of operation and instructions for handling the resulting data storage mechanisms; and computer workstation data safety. This latter should include using a password-protected screensaver and a clean desktop policy; regular logging off when leaving the room; keeping passwords safe, or replacing them by hardware-based identification (smartcards, fingerprint readers); keeping professional and private computer data separated;

scheduling regular computer system maintenance, including hardware checkups and the replacement of faulty or high-risk modules, operating system, and other software updates; use of licensed anti-malware software, including antivirus, firewall, and mail-screening modules. Special attention must be paid to the importance of routine digital signature and electronic time stamp technology application, both for signing internal medical records and for sending medical documents outside of the primary care physician's practice. It is also worth keeping in mind that, in Poland, a digital signature on an electronic document is treated the same in law as a handwritten signature on a paper documents, as only a digital signature with electronic timestamp allows the subsequent determination of authorship, time of creation or modification, integrity, and authenticity of an electronic document [10]. Unfortunately, acquire both a certified digital signature and electronic timestamp service can be quite expensive in Poland, as they are provided not by state but by several state-licensed commercial institutions [20].

Legal obligations to secure medical data

Current laws on medical data security, including those of significance to primary care physicians, are scattered across the Polish legal system and have been evolving dynamically over the last decade. At their root lies the Polish parliament's Act on Personal Data Security [21]; their trunk is the Act on Patients' Rights and the Ombudsman for Patients' Rights [22]; and the main branches are the Act on the Professions of Physician and Dentist [23], the Act on Medical Treatments [24], the Act on Information Systems in Healthcare [25], the Act on Trust Services and Electronic Identification [26], and the Criminal Code [27]; the most important among the many leaves are the Minister for Health's Ordinance on the Kinds, Extent, and Templates of Medical Documents and on Means of Processing Them [28], the Minister for Justice's Ordinance on the Kinds and Extent of Medical Documentation in Medical Treatment Facilities for Detainees and Means of Processing Them [29] and the Minister for Internal Affairs and Administration's Ordinance on the Kinds, Extent, and Templates of Medical Documents in Medical Treatment Facilities Created by the Minister for Internal Affairs Relevant to Internal Affairs and Means of Processing Them [30]. An important role in medical data security is also played by the codes of ethical conduct for members of Polish medical professions, especially physicians [31], but also nurses and midwifes, pharmacists and paramedics. These are not part of the Polish statutory legal system of common application. Most of those regulations have been subjected to amendments of various sizes in the recent years but, at the same time, they have all earned themselves a place in the teaching programs for both medicine students and specialist trainees, as well as among several medical conferences lecture topics and in numerous scientific medical publications.

The personal data security revolution is coming

Since 2004, the Polish legal environment has been shaped by the acts of European Union institutions. Several of these are relevant to our topic, but the most important remains Directive 95/46/WE(EC) of the European Parliament and Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [32]. However, after over 20 years of application it will be replaced on 25 May 2018 by a new Regulation (EU) 2016/679 of the European Parliament and 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 [33]. It is definitely worth becoming familiar with this regulation, as it contains numerous solutions crucial to medical data security of patients, as well as to ensuring medical professionals' safety from draconian administrative penalties. According to Article 2, the Regulation [33] "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"; a *filing system* here means "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis"; and *processing* is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Article 4 of the Regulation [33] contains several definitions more relevant to practice: An *identifiable natural person* is a person who "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". The term *data subject* refers to "an identified or identifiable natural person". For the purposes of the Regulation [33], *personal data* means "any information relating to data subject". It is obvious that the data systems of a primary care practice, computerized or not, fit into the Regulation's [33] scope of interests.

Basic rules to be followed in processing personal data

The Regulation [33] specifies several pivotal rules that apply to personal data. Article 5 gives them as lawfulness, fairness and transparency; data minimization; accuracy; integrity and confidentiality; purpose limitation; storage limitation; and accountability. The first of these means that personal data should be "processed lawfully, fairly and in a transparent manner in relation to the data subject". The data minimization rule means that it is permitted to process only personal data that are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"; the following rule requires that personal data are "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". The next rule specifies that the personal data are "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures". Purpose limitation means that the personal data can be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes", and the storage limitation rule means the personal data need to be generally "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". Both of the last two rules can be applied with the exception of limited "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes". The final rule from the listed means that compliance with all these rules must be capable of being demonstrated by a person responsible for the data processing. Following all those rules demands a great deal of highly organized effort and accepting a highly active attitude towards processed personal data and leaves only a small margin for the inevitable errors.

Limitations on processing data concerning health

The term *data concerning health* used in Article 4 of the Regulation [33] describes "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", while *genetic data* refer to "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question". Article 9 of the Regulation [33] states that it is prohibited to process these types of data, similarly to the cases of personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of biometric data for the purpose of uniquely identifying a natural person or data concerning a natural person's sex life or sexual orientation. However this limitation does not apply to medicine-relevant situations when "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services", "processing is necessary for reasons of public interest in the area of public health", "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent", "processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity", "processing relates to personal data which are manifestly made public by the data subject", or "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where law provide that the prohibition of data processing may not be lifted by the data subject". Assuming that medical staff members follow the basic rules mentioned earlier, they will generally be on the safe side when working with regular patients and in emergencies.

Data security measures must be appropriate

Article 32 of the Regulation [33] requires that appropriate technical and organizational measures are implemented "to ensure a level of security appropriate to the risk, including among others as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing". The term *pseudonymisation* is defined as the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". It is worth adding that "in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed". This means accepting an approach different to those associated with earlier similar regulations: instead of outlining the universal minimal data security-related technical and organizational requirements to be met to ensure at least the formal safety of the entity processing the data, the Regulation [33] demands individual ongoing assessment of the existing and expected risks and taking actions to balancing them actively with appropriate countermeasures.

Serious consequences for data security infringement

Article 82 of the Regulation [33] guarantees the right to compensation, stating that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation for the damage suffered" from the entity responsible for personal data security. Nevertheless, its Article 83 also allows the imposition on those entities of administrative fines, depending on: "the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the damage suffered by data subjects; the degree of responsibility taking into account technical and organizational measures implemented; any relevant previous infringements; the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; the categories of personal data affected by the infringement; the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the responsible entities notified the infringement; compliance with any measures that have previously been ordered against the responsible entity concerned with regard to the same subject-matter; adherence to approved codes of conduct or approved certification mechanisms; and any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement". Such an administrative fine "shall in each individual case be effective, proportionate and dissuasive" and can be imposed "up to 20,000,000 Euro, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher". In this context, it is no surprise that the Polish General Inspector of Personal Data Security has already placed on its official website a bright red timer counting down the time to the moment of the Regulation's [33] coming into power, to forewarn all interested entities, with the hops that the preparations will begin well ahead of the deadline [34].

Guidelines for primary care physicians

It is important for medical professionals to remember that the increasingly common electronic medical records (EMRs) are subject to threats that are different in nature from those that apply to the conventional and well-known paper documents. As with any other computer system, EMRs can be attacked in many different ways, including using social techniques, breaking through physical barriers, destroying computer hardware, and overcoming software-based security measures. In order to keep medical data secure, primary care physicians need to continuously educate staff of all levels; acquire the professional help of IT specialists in computer system setup and maintenance; and repeatedly assess and reassess the existing threats and the accuracy of the measures that can be taken to prevent the risks. Paradoxically, the low level introduction of EMRs can be considered a major factor securing patients' medical data in Poland. When Regulation (EU) 2016/679 comes into power, it will mean increased demands in the field of medical data security and, as a result, elevated legal, formal, and financial risks associated with possible infringement. These should be taken seriously into account as soon as possible when planning any adjustments to or investments into primary care facilities.

Source of funding: This work was funded by the authors' resources.
Conflict of interest: The authors declare no conflict of interests.

References

1. Kanecki K, Nitsch-Osuch A, Tyszko P. Health-Related Quality of Life or Quality of Medical Service? Current challenges for family doctors. *Fam Med Prim Care Rev* 2016; 18(3): 382–386.
2. Tyszko Z, Nitsch-Osuch A, Mińko M, et al. Primary health care tasks in implementing the main operations of public health. *Fam Med Prim Care Rev* 2016; 18(3): 394–397.
3. Tomczyk J. CHIP pyta analityków o WannaCry w polskim Internecie [cited 27.06.2017]. Available from URL: http://www.chip.pl/news/bezpieczenstwo/wirusy/2017/05/wannacry-niewielkie-zagrozenie-dla-polski (in Polish).
4. Smith A, Smith S, Bailey N, et al. Why 'WannaCry' malware caused chaos for National Health Service in U.K. [cited 27.06.2017]. Available from URL: http://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126.
5. Susło R, Trnka J, Drobnik J. *Dokumentacja medyczna jako niezbędny element w działalności lekarza rodzinnego.* In: Steciwko A, ed. *Medycyna rodzinna – co nowego?* T. 1. Wrocław: Wydawnictwo Cornetis; 2010: 94–96 (in Polish).
6. Susło R, Trnka J, Drobnik J, et al. *Nowe niebezpieczeństwa wynikające ze zmian w sposobie prowadzenia dokumentacji medycznej*. In: Steciwko A, Drobnik J, eds. *Wybrane aspekty formalnoprawne w podstawowej opiece zdrowotnej*. Wrocław: Akademia Medyczna; 2008: 65–76 (in Polish).
7. Susło R, Świątek B. Ochrona danych medycznych a opiniowanie sądowo-lekarskie. *Arch Med Sad Kryminol* 2005; 55(4): 314–318 (in Polish).
8. Susło R, Trnka J, Drobnik J, et al. Nieprawidłowości dotyczące wewnętrznej dokumentacji medycznej. *Przew Lek* 2008; 1: 275–280 (in Polish).
9. Drobnik J, Susło R, Trnka J, et al. Nieprawidłowości dotyczące zewnętrznej dokumentacji medycznej. *Przew Lek* 2008; 1: 270–274 (in Polish).
10. Susło R, Drobnik J, Trnka J, et al. Potencjalne zagrożenia związane z prowadzeniem dokumentacji medycznej w postaci elektronicznej. *Fam Med Prim Care Rev* 2007; 9(3): 866–870 (in Polish).
11. Susło R, Trnka J, Drobnik J, et al. Sposób sporządzania dokumentów medycznych jako przyczyna błędu opiniodawczego. *Fam Med Prim Care Rev* 2009; 11(3): 506–508 (in Polish).
12. Susło R, Trnka J, Drobnik J. *Prawidłowe dokumentowanie komunikacji lekarza z pacjentem oraz osobami z jego otoczenia i jego rola w wyjaśnianiu podejrzenia popełnienia błędu medycznego.* In: Steciwko A, Barański J, eds. *Porozumiewanie się lekarza z pacjentem i jego rodziną: wybrane zagadnienia.* Wrocław: Elsevier Urban & Partner; 2012: 223–233 (in Polish).
13. Susło R, Drobnik J. Dokumentacja lekarza rodzinnego jako źródło dowodów w przypadku przestępstw przeciwko życiu i zdrowiu. *Przew Lek* 2009; 1: 262–265 (in Polish).
14. Drobnik J, Susło R, Trnka J. Rola dokumentacji medycznej POZ w wykrywaniu przypadków przemocy w rodzinie. *Przew Lek* 2009; 1: 266–268 (in Polish).
15. Trnka J, Drobnik J, Susło R. Badania i sporządzanie dokumentacji medycznej w przypadku ofiar przestępstw na tle seksualnym. *Przew Lek* 2009; 1: 257–261 (in Polish).
16. Susło R, Drobnik J, Trnka J. Rozpoznawanie i dokumentowanie przypadków przewlekłej intoksykacji wśród pacjentów podstawowej opieki zdrowotnej. *Przew Lek* 2010; 2: 180–183 (in Polish).
17. Susło R, Trnka J, Drobnik J. Zastosowanie dokumentacji medycznej na potrzeby opiniowania w sprawach wypadków komunikacyjnych. *Fam Med Prim Care Rev* 2009; 11(3): 767–772 (in Polish).
18. Trnka J, Susło R, Drobnik J. *Aspekty etyczne komunikacji lekarza z pacjentem i personelem medycznym oraz podstawowe zasady obowiązujące przy komunikacji z użyciem tradycyjnych oraz nowoczesnych środków przekazu.* In: Steciwko A, Barański J, eds. *Porozumiewanie się lekarza z pacjentem i jego rodziną: wybrane zagadnienia.* Wrocław: Elsevier Urban & Partner; 2012: 234–243 (in Polish).
19. Susło R, Trnka J, Drobnik J, et al. Specyfika stosowania systemów informatycznych w działalności usługowej, naukowej i dydaktycznej instytucji medycznych. *Fam Med Prim Care Rev* 2008; 10(3): 696–698 (in Polish).
20. Podpis elektroniczny [cited 27.06.2017]. Available from URL: https://e-podpis.online/pol_m_Podpis-Elektroniczny-218.html (in Polish).
21. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133, poz. 883, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download;?id=WDU19971330883&type=3 (in Polish).
22. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009 nr 52, poz. 417, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20090520417&type=3 (in Polish).
23. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. 1997 nr 28, poz. 152, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU19970280152&type=3 (in Polish).
24. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. 2011 nr 112, poz. 654, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20111120654&type=3 (in Polish).
25. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 nr 113, poz. 657, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20111130657&type=3 (in Polish).
26. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016, poz. 1579) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20160001579+2016%2410%2407&type=1 (in Polish).
27. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88, poz. 553, with subsequent amendments) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU19970880553&type=3 (in Polish).
28. Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015, poz. 2069) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20150002069&type=2 (in Polish).
29. Rozporządzenie Ministra Sprawiedliwości z dnia 26 lutego 2016 r. w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania (Dz.U. 2016, poz. 258) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20160000258&type=2 (in Polish).
30. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 lutego 2016 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. 2016, poz. 249) [cited 27.06.2017]. Available from URL: http://isap.sejm.gov.pl/Download?id=WDU20160000249&type=2 (in Polish).
31. Uchwała Nadzwyczajnego II Krajowego Zjazdu Lekarzy z dnia 14 grudnia 1991 r. Kodeks Etyki Lekarskiej (with subsequent amendments) [cited 27.06.2017]. Available from URL: http://www.nil.org.pl/__data/assets/pdf_file/0003/4764/Kodeks-Etyki-Lekarskiej.pdf (in Polish).

32. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [cited 27.06.2017]. Available from URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1.
33. 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 [cited 27.06.2017]. Available from URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
34. Generalny Inspektor Ochrony Danych Osobowych [cited 27.06.2017] Available from URL: http://www.giodo.gov.pl/ (in Polish).

Tables: 0
Figures: 0
References: 34

Received: 02.07.2017
Revised: 04.07.2017
Accepted: 11.08.2017

Address for correspondence:
Robert Susło, MD, PhD
Zakład Gerontologii
Katedra Zdrowia Publicznego UM
ul. Bartla 5
51-618 Wrocław
Polska
Tel.: +48 71 347-90-29
E-mail: robertsuslo@gmail.com