e-ISSN 2083–4640
ISSN 1507–1367

REVIEW ARTICLE

Reports of Practical Oncology and Radiotherapy
2021, Volume 26, Number 6, pages: 833–838
DOI: 10.5603/RPOR.a2021.0138
Received: 24.11.2021
Accepted: 26.11.2021

Effective communication between hospital staff and patients in compliance with personal data protection regulations

Mirosława Mocydlarz-Adamcewicz[1, 2]

[1]Electroradiology Department, Poznan University of Medical Sciences, Poznań, Poland
[2]IT Department, Greater Poland Cancer Centre, Poznań, Poland

ABSTRACT

Secure communication between patients and health care facilities is especially important In 2016, the European Union (EU) introduced a new regulation — the General Data Protection Regulation (GDPR), applicable in all EU member states — aimed at improving protection of personal data. The GDPR provides broad guidelines on data protection, but generally lacks specific details. Consequently, although member states must comply with the GDPR, there is some flexibility to develop new regulations to suit national characteristics and practices, especially in key economic sectors, such as health care. The aim of the present article is to discuss the benefits and limitations of legal provisions governing the patient identification (both in-person and remotely). This analysis is based on Polish laws that were recently passed to comply with the GDPR. In some cases, these data protection regulations may be unnecessarily strict, making routine care more difficult than intended by the GDPR. National legislation in Poland imposes strict data protection measures, such as prohibiting the public display of patient names or calling out the patient's name in public. However, after health care personnel around the country criticised many of these measures, the law will be modified to address those concerns. For example, the patient's name can be displayed on a wrist band and on containers with the patient's medicines. Nonetheless, numerous questions still need to be resolved to adapt the general data protection rules to ensure the effective operation of the hospital to avoid problems related to accurate patient identification.

Key words: personal data; patients; hospital care; communication; patient rights; Hospital Information System

Rep Pract Oncol Radiother 2021;26(6):833–838

Understanding personal data protection regulations in the medical setting

In all health care facilities, it is essential to establish reliable, secure communication channels between the patient and the facility. These channels are especially important to properly interpret the signals delivered by patients and to send clear and accurate information. Mutual understanding depends on clear communication to ensure that the individualised treatment plan is performed correctly and the patient is cared for properly. Understanding is also important to build a relationship with the patient based on trust and mutual respect so that the patient feels heard and cared for.

Security of medical data is challenging topic, addressed also in other countries [1–6]. In 2016, the European Union (EU) introduced the General Data Protection Regulation (GDPR) to better protect personal data. This regulation was welcomed by the public, in part due to ongoing reports in the media about the theft of customer data from banks and other institutions. There is no question that the

Address for correspondence: Mirosława Mocydlarz-Adamcewicz, 15 Garbary Street, Poznań, Poland; e-mail: miroslawa.mocydlarz-adamcewicz@wco.pl

health status of an individual should be kept private and not disclosed to others unless lawfully permitted. However, in hospitals and similar health care settings, we must proceed with caution in implementing strict privacy protection measures given that, in some cases, rapid interventions are needed to prevent serious harm or to save lives. In such events, quick access to patient data is often vital.

The GDPR came into force on 25 May, 2018 (after a two-year transitional period), becoming directly applicable in EU member states, with no need for new national legislation. However, the provisions of the GDPR are quite general and lack the specifics needed for routine implementation, leaving room for member states to modify certain aspects of the GDPR in their own data protection laws, especially in economic sectors that require more detailed provisions, such as health care. Nevertheless, under EU rules, national regulations can only clarify protection in specific situations related to data processing, such as specifying the conditions that determine data processing compliance with the law. That is to say, any modifications or new provisions cannot interfere with the European regulation. Nonetheless, the EU did leave some flexibility in the GDPR to strike a balance between personal data protection and effective delivery of medical services, to achieve a reasonable trade-off between patient safety and data protection.

In the present article, I discuss the benefits and limitations of certain provisions governing patient identification, both in-person (at the hospital) and remotely (by internet or telephone). The analysis is based on provisions in Polish law that were passed in accordance to EU regulations. In particular, as I emphasize here, it is important to avoid unnecessarily strict data protection measures in medical procedures, which could make routine care more difficult than necessary under the GDPR.

Identification of patients on hospital grounds

Does open display of the patient's name (e.g., on a wristband) to make it easily visible to hospital staff without specialised tools (e.g., barcode reader) breach personal data protection law?

In accordance with section 36 (3) of the Act on Medical Activity, patients admitted to the hospital are identified with an identification band worn on the wrist (some exceptions eg. for newborns), which allows hospital staff to quickly determine the patient's full name and date of birth. The use of identification bands is only considered problematic by medical staff due to the statutory requirement that these data be recorded in a manner (e.g., barcode) to prevent unauthorised persons from identifying the patient.

Medical personnel point out that lack of easy, open access to basic patient identification data could pose safety implications, potentially leading to patient identification errors as well as increasing the time needed to provide care. In medicine, time is often of great importance, especially in the event of a serious incident, such as fainting. The problem is exacerbated by a lack of proper information technology (IT) tools for reading the barcodes and thus, no possibility of quickly and accurately identifying the patient through a barcode reader integrated into the hospital IT database. In addition, the staff lack experience in sing such tools in their daily work, and the need to carry a barcode reader implies an additional burden. Thus, IT tools, instead of facilitating patient identification and care, may actually represent another difficulty to overcome in order to deliver routine care. Computerization and training is a long-term process, requiring time and significant financial resources. Given these challenges, inaccurate patient identification — due to the lack of openly visible identification data on the wrist band — could negatively impact the patient's health, and potentially even threaten his or her life.

In this context, to ensure protection of the patient's interests in terms of data confidentiality and personal safety, I believe that the changes included in section 63 (3)(a) of the framework of the Act on the Healthcare Quality are justified. The proposed Act calls for open identification of the patient, including first and last name and date of birth, on the identification band. Importantly, these changes to the Act on Medical Activities were proposed in 2018 by the group for personal data protection in health care, which was established by the Ministry of Digital Affairs. This group developed guidelines known as "GDPR in the Health Service", an official document that has been signed and approved by two Polish ministries (Ministry of Health and Ministry of Digital Affairs), as well as by the patient ombudsman and the president of the Data Protection Office. This group and the signatories all sup-

port this measure because they believe that patient health should take precedence over data protection rules, and to reduce the risk patient identification errors in the health care setting. The group has also issued guidelines designed to limit the risk of identification errors, stipulating that, all medical products (including those administered in drips), and other treatments administered to the patient must be marked with the patient's name and surname.

Should both — the barcode and the patient's openly-displayed name — be included on the identification band?

An important question is whether the barcode should be removed from the band altogether (the Act does not address this question). Would the absence of the barcode negatively impact automation and computerisation processes currently in progress? The aim of these automation processes is to facilitate rapid barcode reading, access to the Hospital Information System (HIS) to check patient-related data (e.g. during a medical round), quick access to medical prescriptions (on a mobile device), and the ability to record the time and date of admission of the patient to the operating theatre without needing to manually search for the patient's data, automatic registration in the IT system of medication use at the bedside, and/or for ordering specific diagnostic tests.

Given the factors described above, I believe that eliminating the requirement for a barcode on the identification band would be a step backwards. Eliminating the statutory obligation to use the barcode would lead to the cancellation of projects designed to automatize many processes. Thus, the barcode should remain even as we permit the open display of the patient's full name.

Identification of patients outside of the hospital premises using remote modes of communication

In remote communication (telephone, internet) with the hospital, the first step is to identify the person calling (e.g., the patient, a relative, or an authorised person) and ascertain whether that person is entitled to receive information about the patient's health status. Identification during registration at the hospital or at an outpatient appointment is straightforward and simply requires an ID card. However, remote communication through telephone or the internet involves a whole different set of problems. Verification of identity in a video chat can be achieved by visual inspection of the identification card (without recording the details of the document to maintain confidentiality) or by means of security questions, whose answers are presumably known only to the authorised person. Another potential verification tool is the use of a unique contact number automatically generated by the HIS, which the patient can give to authorised individuals (family members, etc.). This number would be registered in the patient's electronic medical records and be easily accessible by hospital staff, allowing for rapid and efficient communication. However, this system would require accurate and up-to-date contact data (e.g., telephone number, e-mail) in the HIS. Data on the individuals authorised by the patient would need to be included as well and as of July 2021, the hospital is required to verify the data on authorised persons in the patient's account at the health care website.

To ensure that these security measures do not hinder communication, the verification process must be rapid and relatively simple. This is also important to avoid undue stress on patients, who already have enough things to worry about. A simple and straightforward verification process is also vital to avoid generating resistance from staff members, who have limited time to perform remote consultations. Moreover, the focus of the consultation should be on providing the patient with relevant information about treatment and related documentation.

Secure exchange of data regarding patient health status

According to section 27 (1)(4) of the Patient Rights Act, medical documentation may be made available electronically, which, pursuant to section 2 (5) of the Act on Rendering Electronic Services [7], involves technical solutions, including information and communication technology (ICT) devices and software tools (e.g., e-mail) that allow for remote communication and data transmission. Apart from providing access to relevant health care information and documentation through secure websites, which requires setting up an account and identity verification, communication with the patient via

e-mail is unquestionably one of the most effective and common forms of contact. E-mail substantially reduces operational costs by eliminating the costs of sending documents by post, thus saving time for the patient and staff and speeding up document delivery, which is accessible from anywhere with an internet connection.

Medical documentation about health conditions belongs to a specific data category protected by the GDPR. If the content of an e-mail or an attachment contains personal data — including health-related data — that could be used by an unauthorised person to harm the patient in any way, this should be classified as a security breach. Should this occur, the law requires a series of actions, including analysis of the incident, notification to the Polish Personal Data Protection Office and to the individuals whose data has been compromised, and the implementation of corrective actions. In this context, documents and messages sent via e-mail should be handled carefully to ensure the confidentiality of the conversation. All efforts must be taken to ensure that the data cannot be accessed by unauthorised persons, which could violate patient rights, and would also damage the facility's reputation, and possible have financial and legal consequences.

Healthcare facilities are obliged to communicate with patients electronically, but under section 32 of the GDPR, they must evaluate the security risks involved and implement proper technical and organisational measures to mitigate those potential risks. Technical measures include the following: sending correspondence to an authorised recipient; encryption of the communication channel; data encryption (file passwords); and determination of the location of the e-mail servers of the service providers. If these servers are located outside the European Economic Area (EEA), standard contractual clauses must be included in the contracts. These clauses require that the data transfer procedures are in accordance with GDPR regulations to protect the privacy of patients whose data is shared outside the EEA.

According to Polish Personal Data Protection Office, the best and most effective method of securing data is by encryption. If the data are encrypted, then other protective measures (e.g., communication channels or servers) are not needed. Once encrypted, only an authorised person can read the message or files. Even if the data is "intercepted", encryption ensures a very low risk that the data can be read by unauthorised persons, provided that the encryption is sufficiently strong to prevent decryption. The password itself should be given to the recipients by another secure communication channel to minimise the risk of interception. In addition, the facilities should obtain signed authorisation (handwritten or via a qualified electronic signature) from the patient agreeing to receive documentation sent electronically by e-mail. Data loss prevention (DLP) tools may be advisable to prevent the loss of open text data sent erroneously by e-mail. In this case, any attempt to send an e-mail with data defined in the DLP as unauthorised will be automatically blocked. The message will be quarantined and the user who breached the security measures will be blocked and will receive a notification about failure to comply with the Hospital Information Safety policy. These measures greatly reduce the risk of data breaches and the alerts allow employees to intervene to stop any activity that violates these security measures.

SMS notifications: a modern tool for communication between hospital and patient

A simple, convenient approach to facilitate communication between patients and the hospital is telephone text (SMS) notifications, which can be used to send message to patients as well as hospital staff. This is a quick, effective, efficient, and inexpensive tool. Notifications are sent automatically by the hospital's IT system using SMS gateways. SMS messages are handled by the mobile telephone operator, whose business is regulated by telecommunications law, which requires carriers to implement technical and organisational measures to ensure the security and integrity of the network, services, and transmission of messages. These measures should provide a level of security that is commensurate with the risk, utilizing state-of-the-art technology; costs of implementing these measures are also taken into account (section 175). One of these security measures involves a contract between the hospital and the telephone operator including required elements regulating personal data processing by the entity (the hospital) that controls the data.

Unlike e-mail, text messages do not normally contain any data on health status (e.g., results of

medical tests), nor do such messages reveal the identity of the patient. In addition, due to the limited number of characters (approximately 160), text messages only include basic information, such as reminders about an upcoming appointment or diagnostic test, or about a change of date or cancellation of a test. As a result, only the person who receives the SMS and knows about the treatment plan is able to correctly interpret the data. This innovative communication approach ensures that the information directly reaches the patient. SMS-based notifications are a highly useful communication tool; however, the effectiveness of the method depends on the accuracy of the personal data entered into the HIS by hospital staff members. SMS notifications can be also useful to facilitate communication between the staff and hospital, making the flow of information more efficient. In this use case, the notifications may concern, for example, activity related to the IT systems, such as password expiry, or information about a blocked user account.

Controversies surrounding overly rigorous data protection regulations in the clinical setting

In the clinical setting, it is important to strike a balance between safety, efficiency, and data protection. Patients expect to receive health-related data as quickly as possible and staff members often find that restrictive data protection measures requiring IT technology are too time-consuming and complicated, and often unnecessary. This state of affairs is exacerbated by a lack of technical skills among some staff and an incomplete understanding of data security issues. Other questions to consider are legal requirements relative to data security imposed by the hospital, which is the entity responsible for data management and thus responsible for ensuring the accuracy and integrity of patient communication. In this regard, there is an assumption that data protection is as important as the data itself.

The main aim of the GDPR is to harmonise data protection in the EU member states. In Poland, in contrast to many other EU countries, patient confidentiality is more rigorously regulated by guidelines and-national regulations in the medical sector (e.g., the Act on Medical Activities in the field of identification), as evidenced by the strong penalties imposed by the Polish supervisory body. However, when balancing the interests of patients, staff, and the hospital, an important question arises: do security features such as data encryption significantly hinder the provision of health care services? From the patient's perspective, the question is whether patients should accept the risk of disclosing data to unauthorised persons, which could potentially lead to discrimination and/or social exclusion.

Undoubtedly, ensuring patient privacy and protecting personal data is a key element in building patient trust in the staff and health care facility by assuring proper data protection. However, when evaluating the risks involved in processing patient data, the overriding goal must be to protect the patient's vital interests. In other words, we must avoid imposing overly restrictive security measures that could negatively impact the patient's health (and even life) while maintaining a reasonable degree of protection that is commensurate with the risk.

Regulations in the medical sector [8] do not prohibit remote communication, but they do require that compliance with the right to privacy and personal data protection stipulated in the GDPR [9], national regulations [10], and in the guidelines on the *Right to Information by Remotely Authorised Persons of July 21,* 2020 [11]. These guidelines were drawn up only four months after the beginning of the pandemic in Poland; at that time, health care facilities were required to develop their own procedures to assure data confidentiality when using IT tools (video chat, telephone, or dedicated websites) to conduct remote consultations with patients.

Due to the pandemic, the need to remotely identify patients now forms part of routine practice. In many cases, conventional, in-person access to medical services at medical facilities has been limited or even completely interrupted during the COVID-19 pandemic. Remote communication, based on the efficient and secure identification of the patient, provides access to health care service and also lowers the risk that any personal health care data will be shared with an unauthorised person. Remote consultations eliminate the need for patients to visit the hospital, thus limiting personal contact between patients and hospital staff. In turn, this reduces the risk of disease spread while maintaining the standards of care (in terms of comfort, convenience, safety, and privacy) in line with tradi-

tional health care delivery. In addition, the use of carefully conceived special measures to accurately identify patients remotely minimises the risk that medical personnel could be held criminally liable for breaching data protection laws.

Conclusions

The broad nature of the EU GDPR regulations allows for individual countries to draw up national regulations that strike a balance between personal data protection and effective delivery of medical services.

Poland has recently taken the first steps to draw up and implement national data protection regulations. However, these regulations are quite strict and do not allow for the patient's name to be openly displayed or called aloud in any public place. However, after criticism from health care staff, these provisions will be modified to allow names to be displayed openly on an identification band and on all containers with medicines.

Nonetheless, several questions still need to be resolved to adapt the general data protection rules to ensure that they do not unnecessarily encroach on the need for effective hospital functioning to avoid hindering rapid and accurate patient identification.

References

1. Friese KV, Wienke A. [Don't be frightened of the „bad wolf" : The new EU general data protection regulation in hospitals and medical practices]. HNO. 2019; 67(4): 299–303, doi: 10.1007/s00106-018-0563-9, indexed in Pubmed: 30367221.
2. Groenewegen WA, van de Putte EM. [General Data Protection Regulation and medical research: friend or foe?]. Ned Tijdschr Geneeskd. 2018; 162, indexed in Pubmed: 30379505.
3. Qiu H, Qiu M, Liu M, et al. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. IEEE J Biomed Health Inform. 2020; 24(9): 2499–2505, doi: 10.1109/JBHI.2020.2973467, indexed in Pubmed: 32071015.
4. Kruse CS, Frederick B, Jacobson T, et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care. 2017; 25(1): 1–10, doi: 10.3233/THC-161263, indexed in Pubmed: 27689562.
5. Nasseh D. The Mishandling of Anonymity in Terms of Medical Research Within the General Data Protection Regulation. Stud Health Technol Inform. 2020; 272: 43–46, doi: 10.3233/SHTI200489, indexed in Pubmed: 32604596.
6. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018; 113: 48–52, doi: 10.1016/j.maturitas.2018.04.008, indexed in Pubmed: 29903648.
7. The Act of 18 July, 2002 on Rendering Electronic Services.
8. The Act of 6 November, 2008 on Patient's Rights and Ombudsman of Patient`s Rights hereinafter UPP, the Act of 15 April, 2011 on Medical Activities, the Act of 5 December, 1996 on Profession of Doctor and Dentist, the Act of 15 June, 2011 on Profession of Nurses and Midwives.
9. The Regulation of the European Parliament and of the Council (EU) 2016/679 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 regulation on data protection) hereinafter GDPR.
10. The Act of 10 May, 2018 on the Personal Data Protection.
11. The guidelines regarding the implementation of the right to information by the persons who are remotely authorised as a result of cooperation of the Ombudsman of Patient`s Rights with the Personal Data Protection Office of 21 July, 2020.