Institute of Mandatory Secrecy and privacy protection

Bc. Miriam Pavelcová

Introduction

I dare to say that the most important institutes for the protection of privacy in the healthcare sector are the management and handling of medical documentation, the provision of information about the patient's health status, and mandatory confidentiality. All these mentioned institutes intertwine with each other precisely through mandatory confidentiality. Protecting data about a patient's health is one of the most important missions of doctors. Confidentiality covers not only purposefully obtained information, but also that accidentally obtained during a conversation with a patient during the performance of medical duties. It is therefore a kind of absolute obligation that can only be limited by law. Its violation can lead to a negative impact on all levels of patient privacy. Be it personal, professional, or social. I dare to say that by violating mandatory confidentiality, the doctor exposes himself to a serious violation of the right to self-determination of the individual.

Mandatory confidentiality

In order to see what is right and what is not, we use rules of conduct and ethical standards. Not only in the healthcare sector, but this behavior towards patients is also regulated by certain standards. Every these standards have their history, they are related to the development of society and progress in medicine. Norms in the healthcare sector serve not only as instructions for a certain way of acting or behaving, but also strengthen the patient's trust in healthcare professionals and healthcare facilities as such. Even though moral standards in healthcare are not that clearly and concretely defined, they are always based on certain goals and have a purpose, and what are their internal acceptance and external limitations is expected of healthcare professionals. Practical use is the basis. Any ethical codes encourage prudent decision-making, are a certain recommendation and a morally binding norm. However, certain generally binding obligations result from them, which nowadays are also supported by laws. From the position of a patient, each of us encounters situations where a doctor makes unauthorized use of information about a health condition, even if it is common or sensitive data. Of course, any discovery of this information is undesirable. One of the fundamental ethical problems in healthcare, which is mentioned in many ethical and legal standards, is the institution of mandatory confidentiality. Its scope is still debated by the professional public. The institute of mandatory confidentiality evolved from the institute of medical secrecy and was addressed only by the ethical norm. If they compared these two concepts, the concept of medical secrecy is more of a public law character and includes the state's interest in protecting some personal information, in contrast to the concept of confidentiality, which I perceive as private law, as it is more about the protection of a specific interest of a natural person with the aim of protecting this subject from unauthorized information handling. I would like to state here that both of these concepts are intertwined in healthcare. Confidentiality covers not only purposefully discovered information, but also that discovered accidentally during a conversation with a patient while performing the duties of a healthcare worker. It is therefore a kind of absolute obligation that can only be limited by law. Establishing mutual trust between doctor and patient is considered one of the most important features of healthcare. It is obvious that without sufficient trust, the relationship could not work, in case the patient did not trust the doctor, he would not provide all the information that could be crucial for his treatment. Another aspect is related to this, namely the effort to protect the patient from unauthorized interference with the privacy and inviolability of his person, as well as human dignity, personal honor, reputation and name, i.e., the protection of basic human rights and freedoms, which is based on

the Charter of Fundamental Rights and Freedoms and the Civil Code and the prevention of discrimination against the patient on the basis of his social, national or ethnic origin and health status. (NCSL, 2011)

The Value and Importance of Health Information Privacy

Ethical health research and privacy provide many valuable benefits to our company. Health research is fundamental to improving human health and health care as such. Protecting patients involved in research from harm and preserving their rights is essential to ethical research. The main reason for protecting patients' personal data is to protect patients' interests. On the other hand, the main reason for collecting personal data and health information is to benefit the company. It is important to mention that privacy also has value at the societal level, as it allows more complex activities, including public health research, to be carried out in a way that protects the dignity of individuals. At the same time, it can be beneficial for individuals. Examples include easier access to new therapies, better diagnostics, and access to more modern technologies. (Aggarwal CC, 2008)

Concepts and value of privacy

Privacy has been defined in many ways over the last century. Warren and Brandeis called it "the right to be let alone". Pound and Freund have defined privacy in terms of an extension of personality or person hood. Westin and others including myself have cashed out privacy in terms of information control. Still others have insisted that privacy consists of a form of autonomy over personal matters. Parent offers a purely descriptive account of privacy. "Privacy is the condition of not having undocumented personal knowledge about one possessed by others". Finally, with all of these competing conceptions of privacy some have argued that there is no overarching concept of privacy but rather several distinct core notions that have been lumped together. Organizations that don't "do privacy" right are at risk—of government enforcement, class action lawsuits, financial ruin, damaged reputation, and loss of customer loyalty. Privacy is now a necessity of doing business. (Ashcroft, 2007, p. 359)

We use the term privacy in many contexts. However, there is no precise definition and there are still gaps regarding the meaning, value, and scope of the concept of privacy. Currently, this term is used to denote various situations such as the right to bodily integrity or to be free from intrusive searches or surveillance. The concept of privacy is specific and takes on different meanings depending on the reasons for the collection, the intentions of the parties involved, politics or cultural expectations. (WHO, 2021, p. 7)

Security of health data

There have been exponential advances in the use of technology in health and healthcare over the last few decades. The medical fraternity has leveraged technology in various ways, including imaging techniques for diagnosis; electronic health records; robotics in surgical procedures; telehealth to diminish barriers and boundaries between patients in terms of distance and time; and, wearables to monitor individuals' health. The use of open data sources is also instrumental in the field of genomics, where data related to genetic makeup, biomarkers and bioinformatics is used to derive better therapeutic solutions. (Saver, 2006)

Many countries have adopted data standards to ensure data safety and security of patients, such as HIPAA (The Health Insurance Portability and Accountability Act). HIPAA is a U.S. federal law that allows individuals to control how their information is used and ensures that data is stored, transmitted and received safely and securely. European projects implement GDPR to restrict access and prevent data leakage. This includes strong password hashing algorithms and internal security reviews amongst others.

Data protection in HISs

An important term in this definition is the word "relating", as it implies both that the data are not owned by the data subject (in the sense of a property right) and that the data may equally relate to more than one person. To give an example, the information that a person is color-blind (something that predominantly affects men) relates equally to the mother as a genetic carrier and to the father of the mother, who will also be color-blind. Consequently, processing such data based on informed consent may require consent from all data subjects the data relate to. Thus, the "data subject" is any identified or identifiable natural person to whom the personal data refer.

Over the last four decades, the standard of regulation in the field of data protection and cybersecurity has very increased. This guidance concentrates less on high-level documents like the EU Charter of Fundamental rights and instead look at the level of regulation closer to professionals operating in the field of HISs. To do this, it is important to distinguish between sector-specific laws regulating the processing of health data, general data protection laws (like the GDPR) and laws that govern the processing of personal data and may have direct or indirect consequences on HISs. Sector-specific laws are important to the extent that they provide clear guidance on the processing of personal data for health purposes and mostly serve as a legal basis for processing activities. Such laws may either address specific public health tasks (par

example such as a cancer registry) or govern the use of health information in a clinical/medical setting (as with electronic health records), with subsequent secondary use of data for public health purposes. In fact, data protection calls for development and implementation of such laws, as these help to achieve a high level of transparency and democratic legitimacy.

As part of the protection of personal data, the administrator must ensure that he only works with specific data. This links to the fundamental data protection principles of data minimization and purpose limitation. For the public health sector, this does not lead to a "default to off" solution, as the default design principle again calls for a balancing of the interests at stake, and for limitation of purposes to vital interests such as protection and promotion of health. We can take for the example the COVID-19 situation, large-scale processing of personal data relating to all citizens may be justifiable and perfectly compliant with the principles, to the extent that such processing is necessary to mitigate the risk of the COVID-19 pandemic. But the principles also call for effective safeguards to ensure that personal data are not used or abused for secondary purposes unless the secondary purpose is equally justifiable. Every public health institutions must also like other institution select partners and service providers carefully – and, in particular, data processors and their subprocessors. IT security and data protection requirements should be part of any relevant tender and procurement process, and the contractual obligations of partners and service providers should mirror all relevant regulatory requirements on the data controller, or any additional requirements a data controller may deem necessary – for example, for the mitigation of reputational risks. (WHO, 2021, p. 11).

Recommended actions:

- Set up a governance process for the development, procurement and implementation of new data processing systems.
- In the light of the processing purpose, develop a strategy on how to minimize implications for data subjects.
- Monitor and audit compliance continuously.
- choosing the right partners and making sure they follow the required standards (WHO, 2021, p. 13)

Digital information

To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. If your patients lack trust in Electronic Health Records

(EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you. Withholding their health information could have life-threatening consequences.

This is the reason why it is so important for you to ensure the privacy and security of health information. When patients trusted you and health information technology (health IT) enough to share their health information, you will have a more complete picture of patients' overall health and together, you and your patient can make more-informed decisions.

In addition, when breaches of health information occur, they can have serious consequences for your organization, including reputational and financial harm or harm to your patients. Poor privacy and security practices heighten the vulnerability of patient information in your health information system, increasing the risk of successful cyber-attack.

In order for patients to trust you, it is advisable to take the following steps::

- Maintain accurate information in patients´ records
- Make sure the patient has access to their records
- Carefully handle patients´ health information to protect their privacy

(Health Information Technology, 2015, p. 8)

Exceptions to the duty of confidentiality and its breach

According to the Act on Health Services, "transmission of information necessary to ensure the continuity of the provided health services" is not considered a violation of mandatory confidentiality in the Czech Republic. In this case, this is the most common exception. As a rule, more health professionals or more service providers are involved in the treatment of a patient - when changing shifts, changing providers or providing data to the patient's general practitioner. Therefore, it is undoubtedly more than necessary for the treatment to work properly that these persons share information about the patient and the course of the treatment. Another exception is "the disclosure of data or other facts if the provider is exempted from confidentiality by the patient, or the patient's legal representative, and if the provider discloses the data or these facts within the scope of the exemption." Here it is appropriate to state that the patient always has the right to revoke this exemption or change its scope. Another exception is disclosure of data or other facts for the purposes of criminal proceedings, interruption or notification of a criminal offense or disclosure of data or other facts by the provider to the extent necessary to protect one's own rights in criminal proceedings.

in the Czech Republic, the provision of information with the consent of the persons to whom the data relate, and the provision of information upon written request, is not a breach of the obligation to maintain confidentiality set out in § 127:

a) Czech National Bank in the exercise of supervision pursuant to this Act,

b) the court,

c) a law enforcement agency,

d) tax administrator for the performance of tax administration,

e) the competent supervisory authority of a Member State or a third country, if it concerns insurance arranged by an insurance company with its registered office in the territory of this State,

f) Office for the Protection of Economic Competition,

g) health insurance companies in the matter of recovery of costs for care covered by health insurance incurred because of illegal actions of a third party against the insured (Czech, 2015)

I cannot help saying that nowadays the institution of mandatory confidentiality has become a legal problem rather than an ethical problem. This is particularly related to the sanction for its violation and the associated criminal liability. Violation of mandatory confidentiality can harm not only the patient, but also the healthcare professional. However, in his book Obligatory Confidentiality, Uherek (2014) points to the fact that, primarily by law, the obligation prevails on the part of the provider, with the patient having rights. And since the patient is in a weaker position in this regard, even though the relationship between the patient and the doctor is supposed to be a private law relationship, he is given a higher level of protection consisting in the obligation of the provider to compensate him for the damage caused in connection with the breach of mandatory confidentiality. I believe that one of the reasons for the violation of mandatory confidentiality on the part of a medical professional is the fact, which I mentioned at the beginning, that many doctors do not know the scope of mandatory confidentiality, that is, what it includes. As an example, we can cite "mass visits", which are a common practice in our healthcare facilities. I believe that it is impermissible for a doctor to talk about a patient's personal diagnosis in the presence of others or to have multiple patients in the office at the same time, unless they expressly agree. In the same way, when addressing patients in front of other patients, the doctor should strongly observe medical ethics. For example, if he were to ask the patient to provide data, he should ensure that the data is received in such a way that their

confidential nature is respected. The Act on Health Services directly states that "the patient has the right to refuse the presence of persons who are not directly involved in the provision of health services." According to the applicable Czech legislation, in such cases every patient who is in a room with other patients should give consent for providing information by a doctor in front of other patients. From my experience, I know that some health service providers interpret mandatory confidentiality very broadly, in such a way that they also include information about a person's hospitalization and disclose this only with the patient's consent, otherwise they fear that they would face a certain violation of the right to protection personal data. Others differentiate between the circumstances of hospitalization - acute or planned and do not find the provision of this information problematic. It takes into account the interest of persons closes to the patient and the right to know this information. In my opinion, this approach is completely relevant from the point of view of personal data protection. The information provided is "true" "not false" and is not a breach of mandatory confidentiality. However, a problem would arise in the case of an unauthorized person's inquiry. If the patient was hospitalized in special wards, for example psychiatry, plastic surgery, or an infectious disease ward. In such a case, the very specialization of these departments is sensitive information, and the health status of the patient can be inferred from it, and the patient to whom this published information concerns could consider this a violation of mandatory confidentiality.

In conclusion, in general, the very fact that a person sought medical help represents a very noticeable invasion of privacy for most of us. In my opinion, this information should be covered by mandatory confidentiality, not only because the law on health services itself calls for it, since the doctor obtained it as a result of the performance of his job, but also from the point of view of internal ethical conviction.

Sources

2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications [online]. In: [cit. 2022-10-22]. Dostupné z: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base

Aggarwal CC, Yu PS, editors. Privacy-preserving data mining: Models and algorithms. Boston, MA: Kluwer Academic Publishers; 2008.

ASHCROFT, Richard Edmund, Angus DAWSON, Heather DRAPER a John MCMILLAN. *Principles of Health Care Ethics* [online]. 2. John Wiley, 2007 [cit. 2022-11-18]. ISBN 97804707134. Dostupné z: https://www.pdfdrive.com/principles-of-health-care-ethics-e185666573.html

Saver R. Medical research and intangible harm. University of Cincinnati Law Review. 2006;74:941–1012.

Sorting Right From Wrong. In: *Www.ncsl.org* [online]. 2011, 2011 [cit. 2022-10-15]. Dostupné z: https://www.ncsl.org/research/ethics/sorting-right-from-wrong.aspx

UHEREK, P., 2014. *Povinná mlčenlivost v souvislosti s poskytováním zdravotních služeb.* Praha: Wolters Kluwer. ISBN 978-80-7478-476-7.

Warren S. and Brandeis L., "The Right to Privacy," The Harvard Law Review, vol. 4 (1890), pp. 193-220