Understanding Privacy Basics in Healthcare

Hrvoje Belani

Ministry of Health, Directorate for e-Health, Zagreb, Croatia

e-mail: hrvoje.belani@miz.hr

Abstract: Achieving and maintaining patient privacy and data protection are inevitable in providing trustworthy healthcare, but often the topics that have not been given enough attention. Understanding privacy basics is crucial for empowering citizens in care, e. g. patients and protégés as well as healthcare workers while providing healthcare. This work covers the following areas and topics of the privacy basics in the context of healthcare: privacy as a human right; short history of privacy; personal privacy protection; privacy and dignity; privacy vs. confidentiality; privacy and availability; cybersecurity vs. privacy; cybersecurity including “CIA triad” and patient safety; privacy in healthcare including legal aspects of data protection. Although this work is suitable for readers with no previous knowledge in privacy, it is useful to relate to everyday-life examples from private and professional surroundings when learning about privacy in healthcare, from both patient and healthcare worker perspectives if applicable. Privacy protection, patient data confidentiality and overall cybersecurity are of huge importance in achieving reliable, trustworthy, safe, and secure environment for both patients and healthcare workers as well as the data they process in any applicable sense.

Keywords: privacy; healthcare; data protection; confidentiality; cybersecurity

Introduction

The term “privacy” has various definitions and aspects it considers, depending on the context and the area of engagement. The Oxford Advanced Learner's Dictionary defines privacy as “the state of being alone and not watched or interrupted by other people”, similar to the Cambridge Dictionary, which defines it as “the state of being alone, or the right to keep one's personal matters and relationships secret”.

Historically, the notion of privacy goes back to the Ancient Greece, where discussions on the distinction between the public sphere of political activity and the private sphere of life relating to family have been attributed to the philosopher Aristotle (384-322 BC). Much later, the first publication advocating privacy in the United States of America was the 1890 article “The Right to Privacy”, defining it as “the right to be let alone”.

Proclaimed by the United Nations (UN) General Assembly in Paris on 10 December 1948, the Universal Declaration of Human Rights (1) in Article 12 states “No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

With technological advancements, privacy concerns also pushed European countries and global organizations to regulate personal data protection, such as Sweden (1973), Germany (1978, 1983), the Organisation for Economic Co-operation and Development (OECD; 1980), the Council of Europe (1981), and the European Union (1995), all the way to the General Data Protection Regulation (GDPR) in 2016, put into force in the EU in 2018.

Privacy Protection

To achieve and maintain privacy, at least to the satisfying point, protection mechanisms have to be put in place, ranging from legal and organizational to technical and behavioural. Defined as the act of covering or shielding from exposure, injury, damage, or destruction, protection aims at valuable assets that need safeguarding, primarily data and information. In the context of privacy, data protection aims at personal data, with health data being a special category of personal data, along with e. g. genetic and biometric data, data about racial or ethnic origin, person's sex life or sexual orientation, political opinions, religious or philosophical beliefs and trade union membership.

As reported by the United Nations Conference on Trade and Development (UNCTAD) at the end of 2021 (2), 137 out of 194 countries (or 71%) had put in place legislation to secure the protection of data and privacy, 9% of countries have drafted legislation, 15% have no legislation and 5% claim no data must be protected. Africa and Asia show different level of adoption with 61 and 57% of countries having adopted such legislations, while the share in the least developed countries in only 48%.

“Privacy protection has been and will continue to be a long-lasting issue with the persistent data collection from various resources, such as medical institutions, social networks, government sectors, etc. The fast proliferation of smart mobile devices accelerates the data collection speed and provides sufficient storage to preserve the datasets, and thereby flourish this big data era, which poses further challenges to privacy protection” (3).

Mainstream privacy protection includes anonymity, clustering-based, differential privacy, cryptography, game theory and machine learning and artificial intelligence methods. Without going further into explanations of each of the methods being researched and implemented in various systems, it is important to point out that personalized privacy protection is an emerging research field, with new and more advanced methods being developed and tested in big data scenarios. Therefore, privacy protection should not only be implemented at the regulation level, but also built-in the organizational procedures and personnel awareness, as well as designed in the technological solutions by so-called “privacy by design” approach, as shown in the Figure 1.

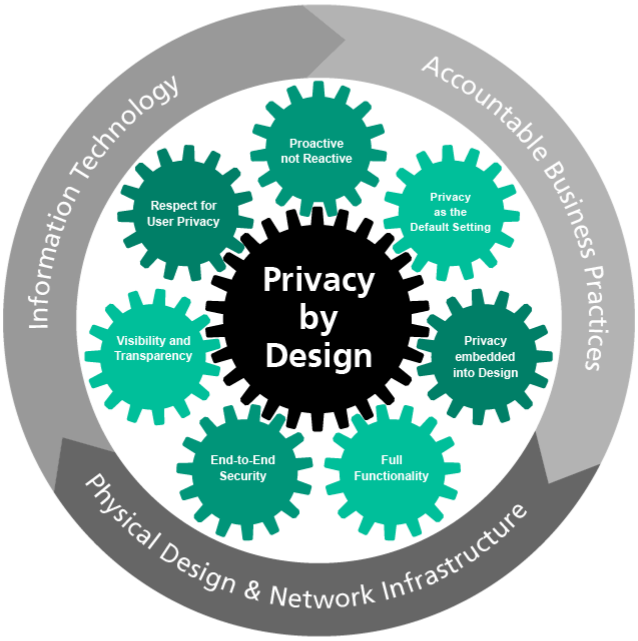

Information Technology
Accountable Business Practices
Physical Design & Network Infrastructure
Privacy by Design
Proactive not Reactive
Privacy as the Default Setting
Privacy embedded into Design
Full Functionality
End-to-End Security
Visibility and Transparency
Respect for User Privacy

Figure 1. Privacy by Design Principles (4)

Privacy and Dignity

We can define dignity as the state or quality of being worthy of honour or respect. In the context of healthcare, where patients deal with mental and physical unease, pain and often shock, dignity is one of the long-established principles healthcare workers always need to stick to, in order to support the well-being of the patients. “Undignified care can have unfavourable impact on the patient’s recovery such as leading to depression and loss of will to live” (5).

“A starting point for thinking about dignity and privacy is the situation of people who have to depend on family or paid carers for intimate, personal care. This may be because of health needs, physical or cognitive disabilities... Respecting people’s privacy is a major part of caring with dignity. In surveys, many people who use services put privacy as their second most important requirement, after safety” (6).

A lot of good practices are already in place at the points of care, practical settings that contribute to maintaining dignity and preserving privacy of patients, e.g., placing curtains round the bed for procedures, examinations, or intimate care, discussing symptoms or treatment discreetly, avoiding accidental exposure, from flapping hospital gowns or rumpled sheets, etc. Basically, every aspect that help patients during healthcare encounters to feel less exposed, vulnerable, judged, anxious and frightened. Therefore, safeguarding and dignity of persons in care are very important part of the patient’s care journey.

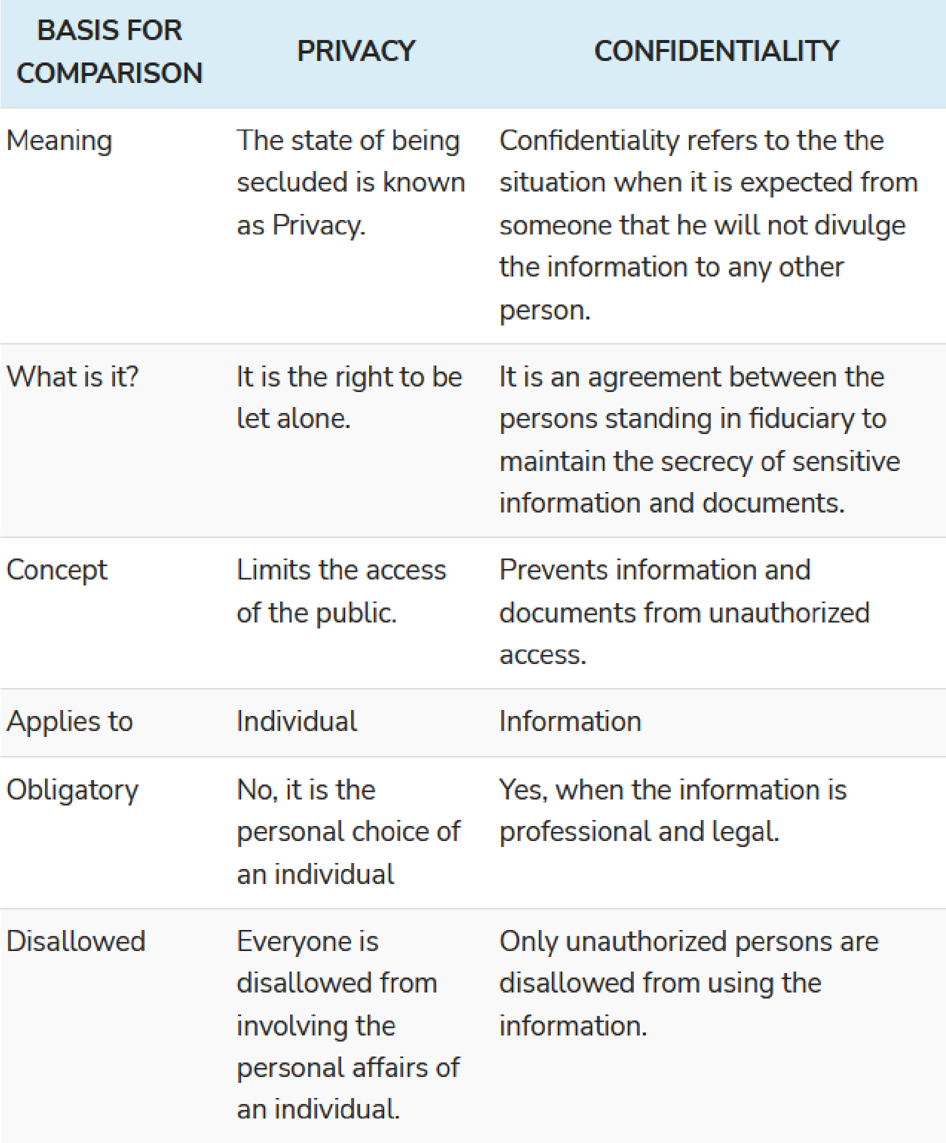
Privacy and Confidentiality

While privacy is a concept related to a person and personal information and data, confidentiality is a concept of ensuring secret information is protected from unauthorized disclosure, no matter if the personal data is involved or not. Confidentiality is about keeping information privileged, about keeping sensitive or classified data from people without the proper clearances. Confidential information is only shared on a “need-to-know” basis. As we can see, confidentiality may help achieving privacy, but they are not the synonyms. Privacy is a state of being secluded and confidentiality is an expectation that someone will not divulge the information to any other person (7).

Confidentiality techniques, like encryption or data access lists, seem necessary to contribute to achieving personal data privacy, but they are not enough for maintaining the full confidentiality of private information. Encryption algorithms may become obsolete over time due to, e.g., the advances of quantum computing and computing power, and the data access lists may become misconfigured if not administered carefully or compromised if not secured properly. Some of the main differences between privacy and confidentiality are shown in the Figure 2 below.

Confidentiality is of huge importance in healthcare when it comes to patients’ data. It builds trust, helps patients get the best care possible, preserves the doctor’s reputation, and it is usually a legal requirement. Some diagnoses, like sexually transmitted diseases and mental health illnesses, still have stigmas attached to them, and keeping them confidential is key.

Confidentiality is also one of the foundational concepts of cybersecurity and is the requirement that most security professionals spend most of their time thinking about. Along with remaining two cybersecurity principles, integrity (I) and availability (A), confidentiality (C) represents well-known “CIA triad”. When it comes to e-health, it is also important to include additional cybersecurity principles, such as authentication (AC), authorization (AZ) and nonrepudiation (NR), which will be explained further in the text.



BASIS FOR COMPARISON	PRIVACY	CONFIDENTIALITY
Meaning	The state of being secluded is known as Privacy.	Confidentiality refers to the the situation when it is expected from someone that he will not divulge the information to any other person.
What is it?	It is the right to be let alone.	It is an agreement between the persons standing in fiduciary to maintain the secrecy of sensitive information and documents.
Concept	Limits the access of the public.	Prevents information and documents from unauthorized access.
Applies to	Individual	Information
Obligatory	No, it is the personal choice of an individual	Yes, when the information is professional and legal.
Disallowed	Everyone is disallowed from involving the personal affairs of an individual.	Only unauthorized persons are disallowed from using the information.

Figure 2. Comparison of Privacy and Confidentiality (7)

Privacy and Availability

Privacy and availability seem to stand in contradiction. With more and more personal health data and information being processed in their primary use – providing immanent care, they could also bring benefit to the healthcare systems with their secondary use – such as in research, medicine development, safety monitoring and policymaking. So, “the dual needs in health to both protect individuals and assure data availability to improve individual and population health call for comprehensive policies governing all entities collecting and using health-relevant information” (8).

To take an example of the National Health Service (NHS) in England, “patients have the right to privacy and confidentiality and to expect the NHS to keep their confidential information safe and secure. Patients also have the right to request that their confidential information is not used beyond their own treatment” (9). Also, “it should be noted that there are exceptional circumstances in which a health or social care professional may be obliged to share confidential patient information in line with the ‘public interest’ or when they are required by law to disclose medical information, regardless of a patient’s consent” (9).

“De-siloed data combinable for delivery, research, and public health are needed for coordinated care, genomic diagnosis, including accurate diagnoses across genetic ancestries, comparative effectiveness research, post-marketing surveillance, data-driven accrual to clinical trials, rare disease research, public health surveillance, early disease detection, development of digital biomarkers to manage patients care at home or to combat a pandemic, and advancing discovery. Sometimes inclusion of entire populations is necessary to ensure generalizability of conclusions across diverse patients and to avoid the non-random statistical biases that would emerge from opt-in models” (8).

Privacy and Cybersecurity

Privacy and cybersecurity are interconnected. With more and more personal information is processed or stored online, privacy protection increasingly relies on effective cybersecurity implementation by organizations to secure personal data no matter what kind of processing takes place – collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The overall aim of cybersecurity is to protect digital assets from being compromised. There are six goals of cybersecurity; three of them are industry-recognized major goals (1–3), and three additional (4–6) that are often neglected (10):

1) Confidentiality (C): keeping information secret.
2) Integrity (I): keeping information correct and reliable.
3) Availability (A): ensuring information is available to the right people at the right time.
4) Authentication (AC): verifying an identity.
5) Authorization (AZ): verifying access to resources.
6) Nonrepudiation (NR): validating the source of information.

Some researchers and experts also add the seventh cybersecurity goal, whose impact is potentially the most critical because the lack of or compromising it could result in injuries, environmental disasters, and even loss of life (10):

7) Safety (S): keeping people protected from physical injury or other health risks.

Safety is introduced to address everyday-life threats posed by the Internet of Things (IoT), the network of physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. In the context of healthcare, for a patient with a connected medical device managing vital medication intake, a potentially mortal risk is occurring if that device is being hacked. Hacks on medical devices such as Insulin Pumps and Implanted Cardioverter Defibrillators (ICD) have been known for several years.

Some of the permanent challenges that occur when combining clinical data from various medical records and health information systems are the consistency and accuracy of clinical data. “Health services and data science researchers recognize that studies leveraging EHR data make a number of necessary assumptions that, when unmet, may lead to spurious results” (11). If not handled carefully, these can also impact patient safety.

The Figure 3 shows how ransomware attacks (to define it shortly, it is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and then demands a payment to unlock and decrypt the data) have impacted patient safety, as reported by the Herjavec Group in their 2021-2022 Healthcare Cybersecurity Report (12).

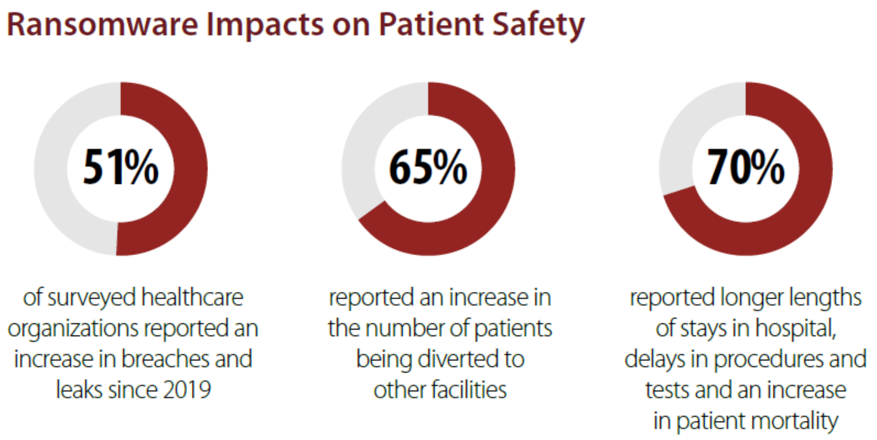


Figure 3. Ransomware Impacts on Patient Safety (12)

Cybersecurity is not one person's responsibility only, but a shared responsibility. It should be built within the organizational culture, set up as a priority business function, as well as properly implemented into technological solutions in place. To illustrate how privacy and cybersecurity must be aligned within organizations, both conceptually and process-wise, the Figure 4 demonstrates different ways that organizations could use:

- the NIST Privacy Framework (13) and
- the NIST Cybersecurity Framework (14)

to better manage privacy and cybersecurity risks collectively.

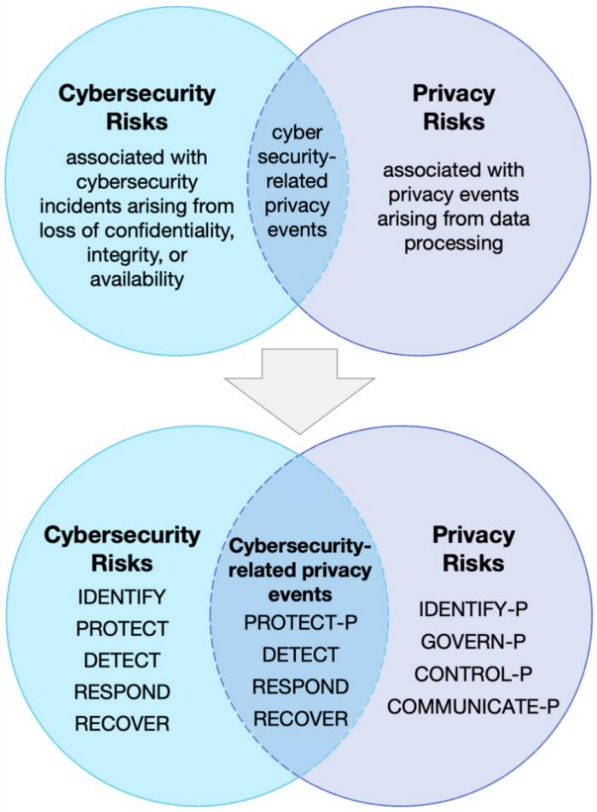

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing
Cybersecurity Risks
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Cybersecurity-related privacy events
PROTECT-P
DETECT
RESPOND
RECOVER
Privacy Risks
IDENTIFY-P
GOVERN-P
CONTROL-P
COMMUNICATE-P

Figure 4. Privacy Framework Venn Diagram (13)

Ensuring Privacy in Healthcare

“Protecting information gathered in association with the care of the patient is a core value in healthcare. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust. Patient privacy encompasses several aspects, including” (15):

- personal space (physical privacy),
- personal data (informational privacy),
- personal choices including cultural and religious affiliations (decisional privacy), and
- personal relationships with family members and other intimates (associational privacy).

As clearly stated in the American Medical Association (AMA) “Principles of Medical Ethics”, physicians must seek to protect patient privacy in all settings to the greatest extent possible and should:

1) Minimize intrusion on privacy when the patient’s privacy must be balanced against other factors.
2) Inform the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware.
3) Be mindful that individual patients may have special concerns about privacy in any or all the above-mentioned areas.

Examples from the two EU Member States and the large third country (16) – Denmark, Estonia and Australia show “it is evident that there are numerous similarities and differences in the type and level of access citizens have to their own health data in the three countries”. Existing national legislation in Denmark and Estonia promote the opt-out system where the citizens' as well as health professionals' access to the personal health data is automatically allowed, but health professionals are only allowed to access it when they are treating the person. “In Denmark, a letter is sent to the citizen if a GP or specialist without any treatment relation has accessed the citizen” (16) and “citizens have the right to block any information from access by health professionals – e.g., specific drugs prescribed or specific diagnosis” (16).

“In Estonia patients are also able to opt out of having their information in the Patient Portal. It is possible to close individual documents, for example information about a visit to a certain health professional or a diagnosis. Alternatively, the patient can close the entire medical record” (16), except for so-called time-critical data (allergies, medical procedures over the past month, last visit to the doctor or hospitalisation, etc.).

In Australia, the system is opt-in and presumes “citizens understand and consent to the specific conditions of the system’s use” (16). “Patients, health care providers and health care provider organisations all need to register for their information to be included”, and “the patients can manage access to their records through the patient portal, that is grant or deny others access” (16).

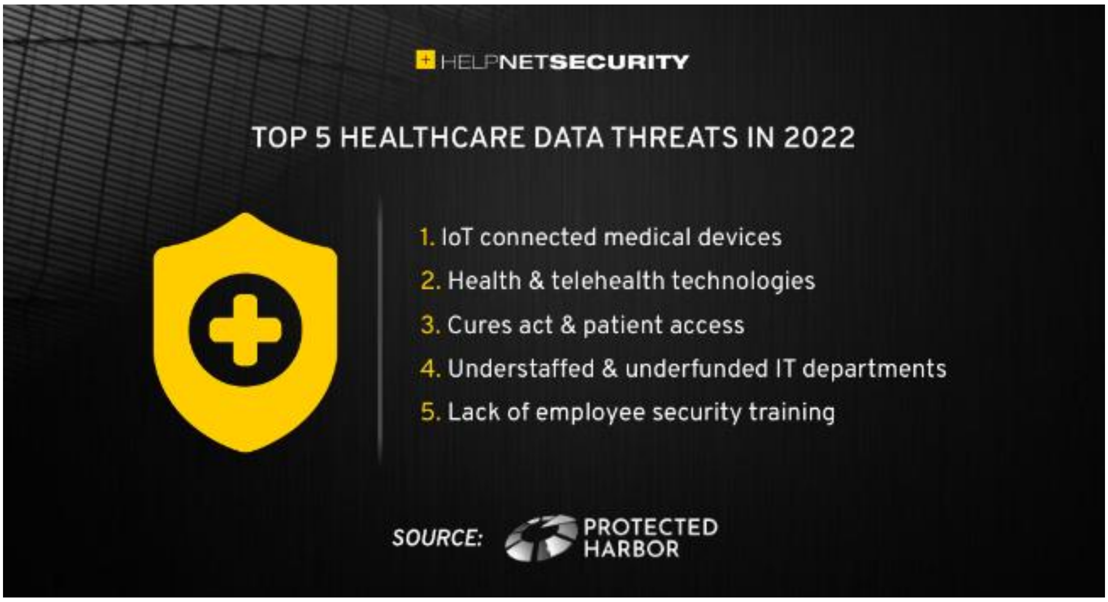
It is important to underline that for all abovementioned countries, it is only possible to close the access to data, which can be reopened, not to erase them. This research has also confirmed that “while current data provides detail on the availability and use of personal health data by citizens, questions still remain over the ultimate impact on patient outcomes of these initiatives” (16).

Healthcare and medical care are evolving as an existing infrastructure and is getting integrated with new technologies. New technologies including electronic health records (EHR) and sensor-based monitoring of in-home patient remotely are being widely implemented. Patient's access to their data is enabled via patient portals and healthcare workers are empowered to regularly monitor health of the patients and save and protect their lives at the earliest. In such heterogeneous environments, cybersecurity and privacy issues emerge from various vulnerabilities present on any level, from information via personnel to the infrastructure.

Improper release of data can happen by both authorized users who access or spread data by infringement of organizational rules intentionally or unintentionally and intruders who hack into an organization’s system. Lack of robust policy or precise organizational procedures may also result in revealing of the patient personal health data to parties that might be in opposition to the patient, again violating the privacy of the patient.

“In order to model the risk to patient safety and patient privacy from cybersecurity causes, one needs a comprehensive method for identifying all the way patient safety and privacy can be compromised by an attacker. This is known as threat modelling. There are many methods of threat modelling available; most of them developed from the perspective of generalized information technology systems. The problem is coming up with an approach for medical device manufacturers that is scalable, manageable, and would stand up to regulatory scrutiny in terms of assuring adequate coverage of the threat space, as it relates to adversely affecting patient safety and privacy… Modelling risk to patient safety from cybersecurity is fundamentally different from modelling risk to patient safety from mechanical, electrical, software, and human factors failure. An alternative risk modelling approach for cybersecurity is needed, with a threat modelling approach driving the identification of risk factors” (17).

To illustrate how wide the threat space is when dealing with healthcare data, top five healthcare data threats in 2022 are shown in the Figure 5.



TOP 5 HEALTHCARE DATA THREATS IN 2022

1. IoT connected medical devices
2. Health & telehealth technologies
3. Cures act & patient access
4. Understaffed & underfunded IT departments
5. Lack of employee security training

SOURCE: PROTECTED HARBOR

Figure 5. Top Five Healthcare Data Threats in 2022 (18)

Legal Aspects of Data Protection

To ensure full compliance with applicable data protection laws and, natural or legal people, e.g. healthcare workers or healthcare organizations, who process personal data, should adhere to the following data protection principles:

- Fair, lawful, and transparent: personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject. Personal data shall not be processed unless permitted by law, based on a preponderant legal interest of the processor or consented to by the data subject.
- Purpose limitation: personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Accuracy and consistency: personal data shall be accurate and consistent and, where necessary, kept up to date.
- Data minimization: personal data shall be adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed.
- Storage limitation: personal data processed for any purposes shall not be kept for longer than is necessary for those purposes.
- Rights of data subjects: personal data shall be processed in accordance with the rights of data subjects as stipulated by the applicable data protection laws.
- Integrity and confidentiality: appropriate physical, technical, legal and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss, alteration (affecting accuracy) or damage to personal data.
- International transfer of personal data: personal data shall not be transferred to a third country or international organization unless that country/organization ensures an adequate level of protection of the rights and freedoms of the data subjects in relation to the processing of personal data.

“Following these principles ensures that… public health authorities are capable of demonstrating that they are fully accountable for their activities, and that the data processing is conducted in a fair and balanced way that affects the right to informational self-determination, or the right to privacy, only to the extent necessary to pursue health-related public interest” (19).

Conclusion

In order to avoid mistakes regarding privacy and tackle data protection challenges properly, both patients and healthcare workers have to get more familiar with the concepts of privacy protection, confidentiality and cybersecurity, as well as how they reflect to healthcare, affecting organizations, processes, people and technology.

Availability, as one of the principles within the “CIA triad”, represents a cybersecurity challenge when it comes to malicious perpetrators or careless users disabling access to the health data. It poses even greater challenge in the broader sense of the term, when it comes to the primary use of health data and information, as well as their secondary use, while the data being siloed and the systems not interoperable enough to combine the data from different reliable sources. Privacy should not be used as an excuse for not having the data available, but should be carefully balanced through legislation, policies, and operations in order to maintain privacy at the satisfactory level and enable decision support by enabling the data availability.

The purpose of this work is to empower the stakeholders in healthcare to become informed how the notion of privacy developed through history, to explain how privacy uses data protection and confidentiality, to make use of seven cybersecurity goals to achieve privacy and to evaluate privacy protection status in healthcare context.

Literatura

1. United Nations General Assembly. Universal Declaration of Human Rights. December 10, 1948, Paris. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights
2. United Nations Conference on Trade and Development (UNCTAD). Data Protection and Privacy Legislation Worldwide. December 14, 2021. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
3. Qu Y, Nosouhi MR, Cui L, Yu S. Introduction. In: Personalized Privacy Protection in Big Data. Data Analytics. Singapore: Springer 2021. Available at: https://doi.org/10.1007/978-981-16-3750-6_1
4. Mangia M. Privacy by Design: theory or methodology? July 19, 2019. Available at: https://digital-health.blog/2019/07/19/privacy-by-design-theoretical-principle-or-development-methodology/
5. Stephen Ekpenyong M, Nyashanu M, Ossey-Nweze C, Serrant L. Exploring the perceptions of dignity among patients and nurses in hospital and community settings: an integrative review. JRN, 2021;26(6):517–537. Available at: https://doi.org/10.1177/1744987121997890
6. Social Care Institute for Excellence in Care (SCIE). Privacy and Dignity in Care. Available at: https://www.scie.org.uk/dignity/care/privacy
7. Surbhi S. Difference Between Privacy and Confidentiality. July 26, 2018. Available at: https://keydifferences.com/difference-between-privacy-and-confidentiality.html
8. McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. Npj | Digit. Med. 2021;4(2). Available at: https://doi.org/10.1038/s41746-020-00362-8
9. Kulakiewicz A and Powell T. Patient Health Records: Access, Sharing and Confidentiality. Research Briefing No. 07103, House of Commons, July 2022. Available at: https://researchbriefings.files.parliament.uk/documents/SN07103/SN07103.pdf
10. Wilson D. Cyber security. The MIT Press essential knowledge series, Massachusetts Institute of Technology, Cambridge, MA, USA, 2021.
11. Singh K, Woodward MA. The Rigorous Work of Evaluating Consistency and Accuracy in Electronic Health Record Data. JAMA Ophthalmol. 2021;139(8):894–895. Available at: https://doi.org/10.1001/jamaophthalmol.2021.2042
12. 2021-2022 Healthcare Cybersecurity Report. Herjavec Group 2021.
13. The National Institute of Standards and Technology (NIST). Privacy Framework. December 2020. Available at: https://www.nist.gov/privacy-framework
14. The National Institute of Standards and Technology (NIST). Cybersecurity Framework. v1.1, April 2018. Available at: https://www.nist.gov/cyberframework
15. AMA. Privacy in Health Care. Available at: https://www.ama-assn.org/delivering-care/ethics/privacy-health-care
16. Nøhr C, Parv L, Kink P, Almond A, Nørgaard JR, Turner P. Nationwide citizen access to their health data: analysing and comparing experiences in Denmark, Estonia and Australia, BMC Health Serv Res 2017; 17(534). Available at: https://doi.org/10.1186/s12913-017-2482-y
17. Ray A. Cybersecurity for Connected Medical Devices. London: Academic Press, Elsevier Inc. 2022.
18. Help Net Security: Healthcare Cybersecurity Report. Q1 2022. Available at: https://www.helpnetsecurity.com/healthcare-cybersecurity-report/
19. WHO. The Protection of Personal Data in Health Information Systems – Principles and Processes for Public Health. Copenhagen: WHO Regional Office for Europe 2020.

Razumijevanje osnova privatnosti u zdravstvenoj zaštiti

Hrvoje Belani

Ministarstvo zdravstva, Uprava za e-zdravstvo, Zagreb, Hrvatska

E-mail: hrvoje.belani@miz.hr

Sažetak: Ostvarivanje i očuvanje privatnosti pacijenata i zaštite podataka neizbježni su u pružanju pouzdane zdravstvene skrbi, ali često i teme kojima se ne pridaje dovoljno pažnje. Razumijevanje osnova privatnosti ključno je za osnaživanje građana u skrbi, npr. pacijenata i štićenika kao i zdravstvenih radnika pri pružanju zdravstvene zaštite. Ovaj rad pokriva sljedeća područja i teme osnova privatnosti u kontekstu zdravstvene zaštite: privatnost kao ljudsko pravo; kratka povijest privatnosti; zaštita osobne privatnosti; privatnost i dostojanstvo; privatnost i povjerljivost; privatnost i raspoloživost; kibernetička sigurnost nasuprot privatnosti; kibernetička sigurnost uključujući „CIA trojku" i sigurnost pacijenata; privatnost u zdravstvu uključujući pravne aspekte zaštite podataka. Iako je ovaj rad prikladan za čitatelje bez predznanja o privatnosti, korisno je pozvati se na primjere iz svakodnevnog života iz privatnog i profesionalnog okruženja kada se uči o privatnosti u zdravstvu, kako iz perspektive pacijenata tako i iz perspektive zdravstvenog radnika ako je primjenjivo. Zaštita privatnosti, povjerljivost podataka o pacijentima i cjelokupna kibernetička sigurnost od velike su važnosti u postizanju pouzdanog, vjerodostojnog, sigurnog i štićenog okruženja za pacijente i zdravstvene radnike, kao i podatke koje obrađuju u bilo kojem primjenjivom smislu.

Ključne riječi: privatnost; zdravstvena zaštita; zaštita podataka; povjerljivost; kibernetička sigurnost