The Art as a Form of Raising Awareness of Data Protection in Healthcare and Medicine

2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) | 979-8-3503-3373-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/MeditCom58224.2023.10266590

Kristina Drusany Starič, MD, PhD
University Medical Centre Ljubljana
Department of Gynaecology and Obstetrics
University of Ljubljana
Medical faculty
1000 Ljubljana, Slovenia
https://orcid.org/0000-0002-5548-4116

Breda Sturm, MA
Artist, Freelance
www.bredasturm.com
1000 Ljubljana, Slovenia
breda.sturm@gmail.com

***Abstract*—Data protection in healthcare and medicine has been an important factor for trust between health provider and patient since the beginning of medicine. In the era of digitalization, the data is not only protected by the health provider, but it is distributed to the digital system where it can be accessible to everyone that has access to the system. The awareness in cybersecurity in Slovenia has started since the beginning of the development of cyber ecosystem. In EU GDPR and in Slovenia ZVOP-2 law is a foundation for data protection and security. The public knowledge of the subject is still very superficial. An interdisciplinary approach to develop proper awareness of the public and robust cybersecurity is crucial. Different approaches, including art can be a crucial point in more efficient informing the general population and improving data security.**

***Keywords*—cybersecurity, data protection, connected health, awareness, electronic records, personal data, digitalization.**

I. Introduction

In the modern healthcare landscape, where advancements in technology are reshaping patient care and medical research, the protection of personal data has emerged as a critical concern. As electronic health records, wearable devices, and telemedicine become increasingly prevalent, it is essential to raise awareness about the importance of safeguarding personal health information. Data protection is a process of protecting digital data, such as health data, especially digital health records. Health data is challenged by many different threats [1]. Patient information can be vulnerable to theft, fraud, terrorism, and natural catastrophes, such as pandemics. The information can be influenced or abused by accident or by the efforts to do harm or take advantage or a person just being nosy. One of the crucial and the simplest improvements is to restrict unauthorized access to digital health records and protect it from hackers [2, 3]. Personal health data, encompassing medical history, treatment plans, test results, and even genetic information, is a treasure trove of insights for both individuals and healthcare providers. This data fuels accurate diagnoses, tailored treatments, and medical research breakthroughs. However, as health data becomes more digitized and accessible, its vulnerability to unauthorized access, breaches, and misuse rises significantly. Raising awareness about the laws for data protection is the simplest way to address the problem. Data encryption, data masking, disaster recovery, and tokenization are a few examples of procedures that fall under the general category of data security [1].

II. Related Work

A. Legislation in European Union

The GDPR, officially known as Regulation 2016/679 (European Parliament and Council, 2016) [4], replaced the Data Protection Directive 95/46/EC (European Parliament and Council, 1995) [5]. Generally, a regulation is a binding legislative instrument that must be applied in its entirety across the EU, which contrasts with a directive that requires implementation into the national laws by the EU's Member States. This change to regulation reflects the importance of further harmonization of data protection legislation within the EU. Yet, albeit being presented as an instrument of strong harmonization of laws, the GDPR does not depart too far from its predecessor: the GDPR still leaves EU Member States a lot of leeway to decide on how to implement it by virtue of so-called 'opening clauses' [6]. An example is the age requirement to give valid consent for services such as social media sites, which can vary among Member States between as high as 16 to as low as 13 years of age. Therefore, the GDPR should be viewed as a further step to stronger harmonization, but data protection laws may still differ in key aspects among the EU Member States. The GDPR is rooted in a dual foundation: on one hand, it aims to facilitate the free flow of personal data; on the other hand, it serves to better protect the fundamental rights of individuals, with a focus on the right to privacy and data protection [7]. In fact, the right to protection of personal data is part of the Charter of Fundamental Rights of the EU [8]. Article 8 of the Charter (2000/C 364/01) clearly indicates that 'Everyone has the right to protection of personal data concerning him or her'.

B. Legislation in Slovenia

The first general (systemic) Personal Data Protection Act of the Republic of Slovenia was adopted in 1990 [9]. It was amended to Personal Data Protection Act – ZVOP-1 [10] adopted in 2004, which is not in force anymore. Since January 26th, 2023, a new Personal Data Protection Act ZVOP-2 is in force [11].

Act ZVOP-2, however, takes into due account also experience and knowledge about the use of the previous ZVOP-1 from 2004, the provisions of Article 38 of the Constitution of the Republic of Slovenia on the human right to the protection of personal data, the existing constitutional review of the Constitutional Court of the Republic Slovenia on the human right to the protection of personal data from 1992 onwards, as well as the provisions still valid, but still not changed, of the Convention on the Protection of

Individuals regarding the automatic processing of personal data.

Objectives of ZVOP-2 are guarantee of as many issues as possible to be regulated or solved by the systemic protection law personal data and thus ensured implementation of human rights in the view of protection of personal data (Article 38 of the Constitution of the Republic of Slovenia), more specifically: guarantee and respect for legal certainty, even in the way that there would be as many provisions as possible, on one place for the effective realization of the personal human rights to the protection of personal data.

C. Data Protection during COVID as an example of natural catastrophe

The model of "ethical trade-offs", which arguably is a central feature in the discussions of data protection and priority setting during the global health emergency. It further highlights and even provides a somewhat acceptable middle ground solution when choosing between innovation that allows better understanding and faces the challenges posed by the pandemic and regulatory compliance [12,13]. Although this solution evidence proves a shift which has been observed towards protecting public health over privacy across many levels, this is always done so long as it adheres to the principles of purpose limitation, proportionality, and transparency [14]. As clearly stated in communication between the European Data Protection Board (EDPB) and the European Commission [15], an enactment of national laws which would result in the temporary limitation of individuals' rights in case of an emergency is not a blanket policy as stipulated under the GDPR. In every specific event, a solid legal framework needs to be implemented which must define in detail the scope, the limited duration of the use of information, disabling of tracking systems and deletion of the gathered data. Further, the mere existence of data protection impact assessments, mandatory under GDPR (Articles 35, 36 and Recitals 89–96), as well as data protection authorities and data protection supervisory bodies should provide solace in that the protection of citizens' privacy interests is paramount and protected [16]. Because of the sensitivity of the subject and the complex nature of ethics in the use of personal sensitive data, a comprehensive review of the ethical standards is needed and practical implementation.

While the urgency of the pandemic underscores the value of data, it also intensifies concerns about data privacy and security. Health records are among the most sensitive personal information, containing details about an individual's medical history, treatments, and potential vulnerabilities. Ensuring the confidentiality and appropriate use of this data is essential to maintain public trust and protect individual rights.

Balancing Act: Public Health vs. Privacy:

Governments and healthcare institutions must strike a careful balance between utilizing health record data for pandemic response and respecting individuals' privacy. Key considerations include:

1) Informed Consent: Transparent communication and obtaining informed consent from individuals before collecting and using their health data are vital. This empowers individuals to make informed decisions about sharing their information for public health purposes.

2) Anonymization and De-identification: Implementing robust anonymization and de-identification techniques can help protect individual identities while enabling the use of aggregate data for epidemiological analysis.

3) Data Security: Employing stringent data security measures to prevent unauthorized access, breaches, and cyberattacks is crucial. Encryption, secure storage, and regular audits are essential safeguards.

4) Limited Use and Retention: Health data should only be used for specific pandemic-related purposes and retained for the necessary duration. Once the crisis subsides, steps should be taken to ensure data is securely and ethically disposed of or retained with explicit consent.

5) Transparency and Accountability: Governments and healthcare organizations should be transparent about their data collection, usage, and sharing practices. Independent oversight and accountability mechanisms can help ensure compliance with data protection regulations.

Pandemic underscores the delicate interplay between public health imperatives and personal data protection. As we navigate this challenging landscape, it is essential to ensure that the collection, usage, and sharing of health record data are conducted ethically, transparently, and securely. By upholding these principles, we can harness the power of data-driven responses to the pandemic while safeguarding individual rights and privacy in an increasingly digital world.

D. Is there awareness?

Just as a doctor-patient relationship is built on trust, so too is the confidentiality of health data. Patients must be assured that their sensitive information remains private. Breaches in healthcare data can lead to dire consequences, including identity theft, fraudulent medical billing, and even the compromise of a patient's mental and emotional well-being. The ethical responsibility of healthcare professionals to protect patient data is paramount. Upholding patient confidentiality not only respects individual rights but also ensures a foundation of trust between patients and providers. This trust is a crucial element in effective medical care, empowering patients to share accurate information about their health and lifestyle. A cross-sectional study was directed between May and June 2019 on a sample of 229 nurses working in the health care area. An electronic questionnaire was constructed, evaluated for its validity and reliability. The participants were volunteers from nursing professional pages on social media. The study indicated that the nursing staff who participated were not fully informed about the GDPR and its implementation. The level of awareness of the participants was found to be related to the age, the employment in the private health sector, the education level, the position of responsibility and the years of experience [17].

The always lingering question of data protection in healthcare was studied through comparison of three surveys. The results from the surveys conducted in 1993, 1995, and spring 1998 show that a deeper understanding of data protection is slowly penetrating the nursing profession [18]. On the other side, non-trusting in the data protection the donors of the data have problems giving the data for the research and that for the researchers are limited.

The public must be aware that their data is protected by the law.

Research shows that concerns about privacy are affecting patients' willingness to share their medical history [19]. For donors to be able to make an accurate decision about their willingness to share medical data and to build trust in health actors using the data, a precise understanding of what data anonymity means is essential. Otherwise, a decision to share data and subsequently donor's trust is based on false assumptions [20].

Several factors have contributed to the heightened awareness of personal data protection:

1) High-Profile Data Breaches: Numerous high-profile data breaches involving well-known companies and institutions have highlighted the vulnerability of personal data. These incidents have drawn significant media attention and public concern, prompting discussions about data security.

2) Data Protection Regulations: The introduction and enforcement of data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), have played a crucial role in raising awareness. These regulations establish strict guidelines for how organizations collect, process, and protect personal data.

3) Media Coverage: Media outlets often cover stories related to data breaches, privacy violations, and discussions about data protection laws. These stories contribute to public awareness and understanding of the importance of safeguarding personal information.

4) Educational Campaigns: Governments, non-profit organizations, and advocacy groups frequently run educational campaigns to inform individuals about their rights and responsibilities concerning personal data protection. These campaigns aim to empower individuals to take control of their data.

5) Online Privacy Tools: The availability of privacy-focused tools, such as browser extensions, VPNs (Virtual Private Networks), and encrypted messaging apps, has helped individuals take proactive steps to protect their personal data online.

6) Corporate Initiatives: Many companies are implementing stronger data protection measures and promoting transparency in how they handle customer data. This includes providing clearer privacy policies, consent mechanisms, and options for data control.

7) Social Media and Tech Industry Scrutiny: Public discussions about how social media platforms and tech companies handle user data have contributed to a broader conversation about digital privacy and personal data protection.

8) Growing Concerns: Concerns about surveillance, targeted advertising, and the potential misuse of personal data for political or commercial purposes have fueled public discussions about the need for stronger data protection.

Overall, the increased awareness of personal data protection reflects a growing recognition of the importance of individual privacy and the need for responsible data handling practices by organizations and governments. This awareness is an important step toward fostering a more secure and privacy-conscious digital environment.

III. Proposal for Raising Awareness for Personal Data Protection through the Art

Art has a unique ability to transcend language barriers and evoke powerful emotions. When harnessed to raise awareness about personal data protection in healthcare, it becomes a potent tool for conveying the importance of safeguarding sensitive information. This fusion of creativity and awareness aims to inspire individuals to take an active role in preserving their data privacy within the realm of healthcare.

1) Digital Artistry: In the digital age, personal health data is often stored and transmitted electronically. Digital art can mirror this technological landscape, portraying the delicate balance between connectivity and security. Imagery of intertwined circuitry and data streams can symbolize the interconnectedness of healthcare information, urging viewers to contemplate the need for robust data protection measures.

2) Metaphorical Masterpieces: Artists can craft metaphorical compositions that draw parallels between data security and the protection of physical well-being. A canvas adorned with shields, locks, and barriers can serve as a visual representation of the layers of protection required to safeguard personal health information.

3) Emotive Portraiture: Portraits capturing the expressions of patients, doctors, and nurses can evoke empathy and intrigue. By depicting moments of trust, care, and shared responsibility, artists can emphasize the vital role each stakeholder plays in upholding data security within the healthcare ecosystem.

4) Collage of Concerns: Collages can weave together elements of technology, healthcare settings, and privacy symbols. These collages can embody the multifaceted nature of data protection, inviting viewers to delve deeper into its nuances and significance.

5) Vivid Symbolism: The symbolism of a locked padlock, a vigilant eye, or an embracing shield can serve as powerful motifs to convey the message of safeguarding personal data. These symbols can be interwoven with medical tools and settings to emphasize the integration of data protection within healthcare.

6) Interactive Installations: Immersive installations that invite viewer participation can elevate awareness to a tactile level. For instance, visitors might navigate a maze representing data protection challenges while discovering visual cues that underscore the importance of secure data management.

7) Healing Hues: Colours can evoke emotions and associations. Incorporating healing tones such as calming blues and soothing greens can create a sense of serenity while underscoring the importance of maintaining a peaceful equilibrium between health and data privacy.

8) Storytelling through Art: Narrative artworks can tell compelling stories of individuals whose lives have been positively impacted by data protection measures. These stories can humanize the concept of data security, making it relatable and motivating viewers to take similar precautions.

Regenerate protection and security awareness should reach the broader public as much as possible. To address the

broader audience besides the usual analogue or digital media channels (like newspapers, TV, websites etc.), the information could be shared on complementary platforms such as art.

We propose art projects, installations, and performances for interactive public awareness of the subject.

Personal Data Protection Art – PDPA (Umetnost varstva osebnih podatkov – UVOP) Project [21] in various variations addresses the 21st century digital era challenges of ensuring human rights and fundamental liberties already defined in 1968, in the General Assembly — Twenty-third session 2450 (XXIII) — Human rights and scientific and technological developments [22]. As an artwork in progress cautions on several cyberspace challenges.

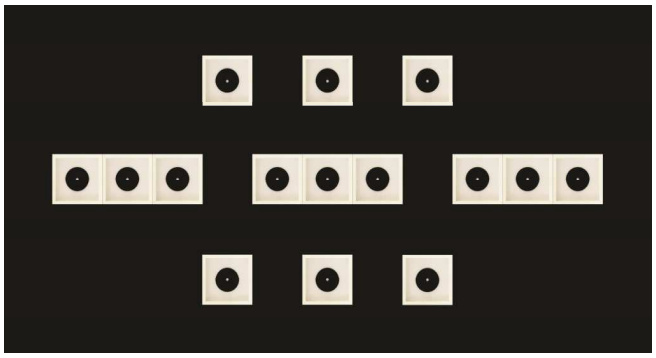

Fig 1. Artwork SOS emphasizes the importance of data security. Data should be stored on different platforms to be protected [23].

Example of art stressing importance of digital data is artwork titled SOS – Written Secrets (PDPA), currently presented in an annual exhibition by The Union of Slovene Fine Arts Associations, in Slovene: Majski Salon 2023 – Misterij Gea (16. 6.–16. 8. 2023), in a mixed technique, presenting the inscription SOS that consists of 15 written secrets elements in the spaces corresponding to the Morse Code composed of framed CDs and DVDs containing medical data (US images, MRI images, X ray images etc.), the contents of which can no longer be read as this digital data carrying devices are becoming obsolete. As a carrier of protected data transformed into permanently hidden content, it thus becomes the former carrier of information that we wrote/burned to CD/DVD. By destroying the carrier as a source of information, it acquires a new artistic role, and thus the written information become Written Secrets, in Slovene: Zapisane skrivnosti, which appear in various settings formations and transformations of the UVOP Project.

With the general disuse of CDs/DVDs remains an extensive heap of non-degradable waste. Artwork SOS – Written Secrets as well highlights the issues of environmental protection and waste recycling of numerous digital content carriers that have accumulated in recent decades.

Medical data is stored on several different media, in case of deletion, intentional or accidental, they can serve as a backup and thus preserve medical documentation**.**

The essence of information privacy is to ensure that an individual keeps information about himself because he does not want others to be privy to it. This is the subject of Article 38 of the Constitution of the Republic of Slovenia, which defines the protection of personal data as a human right [24].

Art can also point to all this. The artist decides whether to present protection or exposition of the personal data in artwork.

The project stressing The Art as a form of raising awareness of Personal Data Protection was launched in 2022 as a work in progress and it has no date of expiry. It aims at informing a broader public on the issues of the human rights and personal liberties in a digital era.

We propose exhibitions in the gallery spaces of the Health Institutions and Hospitals. Consequently, this issue shall reach doctors and all medical staff as well as the patients. We also propose exhibitions in public and private galleries, to get wider audience.

We expect the proposed exhibitions of visual art will be a great tool for furthering the ideas of human rights and fundamental liberties in AI environment introducing everyday life, and a good basis for organizing panel discussions about Personal Data Protection Awareness in health care and other fields of human activity.

IV. Conclusion

In a world where data flows ceaselessly through the digital conduits that underpin modern life, the question of personal data security within the healthcare landscape becomes not just a concern, but an imperative. This imperative extends its influence into both the routine and the extraordinary, demanding our unwavering attention regardless of the circumstances. The act of safeguarding sensitive information is not a passive endeavour; it is an ongoing, dynamic process that requires constant vigilance and proactive measures.

At the heart of this imperative lies the realm of health and medicine – a domain where data security resonates with a gravity that transcends its technical implications. It embodies a holistic approach to wellness, where every bite of information holds the potential to influence diagnoses, inform treatment plans, and contribute to the pursuit of a healthier, more productive life. As we stride forward into an era of digital health records and telemedicine, the need for preserving the sanctity of personal health information has become a call that should echo within every corner of society.

The architect of this sanctuary is a tapestry woven with the threads of regulations and laws, a tapestry that should be interwoven seamlessly into the fabric of medical data protection. From the moment a patient's data is recorded to its eventual utilization in treatment or research, the guardianship of legal standards ensures that each step is characterized by transparency, integrity, and respect for individual rights. These laws should stand as unwavering pillars of assurance, upholding the delicate balance between progress and privacy.

However, the journey towards a safer, more aware healthcare ecosystem extends beyond legislation. It branches out into a landscape rich with diverse strategies for disseminating knowledge about medical data security. Each strategy acts as a beacon, illuminating different paths towards collective enlightenment. Educational campaigns, workshops, and public forums become platforms for demystifying the complexities of data security, arming individuals with the wisdom to navigate this intricate terrain with confidence.

Moreover, the heterogeneous nature of information dissemination demands a versatile approach. The message of data security, like a well-crafted symphony, should resonate through various instruments tailored to reach distinct audiences. Whether engaging with healthcare professionals, patients, policymakers, or the broader public, the harmonious chords of awareness must be struck to create a collective melody of vigilance and understanding.

In this digital era, a symphony of data constantly flows, touching lives and shaping destinies. Amid this symphony, the crescendo of personal data security emerges as a central motif, a refrain that reverberates through ordinary routines and extraordinary challenges alike. It is a call to action, a call to recognize that the act of protecting data is far from passive; it is an unceasing commitment that evolves with the times. With laws as steadfast sentinels and awareness as the guiding star, we can usher in a future where the sanctity of personal health information remains inviolable, enriching lives and safeguarding the foundations of modern healthcare. Security should be addressed from every angle in the ordinary and in extraordinary conditions. We must know that protecting the data is an active process. Data security in health and medicine is an important subject that should reach everyone. The laws should be implemented in every aspect of medical data protection. Different ways of improving knowledge about medical data security are important. Various types of information are reaching different groups of individuals and therefore better awareness of this important subject is crucial. Art has the remarkable power to ignite conversations, provoke introspection, and stir collective action. By harnessing the creative energy of artists, we can paint a vivid tapestry that showcases the delicate interplay between personal health data and data protection. Through visual narratives, symbolism, and interactive experiences, art can elevate awareness of the vital role each individual plays in ensuring the sanctity of their personal health information.

REFERENCES

[1] T. Kunz, B. Lange, A. Selzer. Datenschutz und Datensicherheit in Digital Public Health [Digital public health: data protection and data security]. Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz. 2020 Feb;63(2):206-214. German.

[2] V. Chico, “The impact of the General Data Protection Regulation on health research,” Br Med Bull, 2018, pp.109–118.

[3] A. Brauneck, et al, “Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review, ” J Med Internet Res. 2023, p. 25.

[4] European Parliament and Council. (2016). 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.

[5] European Parliament and Council. (1995). 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. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ (access date: June 17th, 2023).

[6] S. Shaw, “Opening clauses’ and the GDPR - it might not be as easy as we thought, ” 2017 Retrieved from https://www.lexology.com/library/detail.aspx?g¼87f101cb-26ec-4e6b-8184-c5bc2a324513.

[7] O. Lynskey, “ The dual objectives of European data protection regulation, ” In The Foundations of EU Data Protection Law. Oxford, UK: Oxford University Press, 2015.

[8] European Union. (2012). Charter of Fundamental Rights of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri¼CELEX:12012P/TXT (access date: June 17th, 2023).

[9] Official Gazette of the Republic of Slovenia, No. 8/90.

[10] Official Gazette of the Republic of Slovenia, No. 86/04.

[11] Official Gazette of the Republic of Slovenia, No. 163/22.

[12] M. Newlands, et al, “ Innovation under pressure: Implications for data privacy during the Covid-19 pandemic,” Bog Data & Society, 2020, p. 2.

[13] M. Harris, Y. Bhatti, J. Buckley, D. Sharma. “Fast and frugal innovations in response to the Covid-19 pandemic,” Nat Med. 2020;26(06):814–7.

[14] European Data Protection Board EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic 2020. Available from: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-concerning-european-commissions-draft-guidance_en (access date: May 1th, 2020).

[15] European Commission Communication “Coronavirus: Commission proposes a Digital Green Certificate”[2021-03-17] Available from:https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181(access date: June 17th, 2021).

[16] C. Shachar, S. Gerke, E. Y. Adashi, “AI Surveillance during Pandemics: Ethical Implementation Imperatives, ” Hastings Cent Rep, 2020 May;500318–21.

[17] V. Markopoulou, A. Nieri, J. Liaskos, E. Zoulias, A. Mantas, “Nursing Staff's Awareness of Processing Personal Data According to GDPR, ” Stud Health Technol Inform. 2020, pp.237-240.

[18] M. Tallberg, “Data protection--an eternal question, ” Stud Health Technol Inform. 2000;57:248-53. PMID: 10947663.

[19] M. D. Walker, J. Tyler ,W. Eric Ford, R. Timothy Huerta, “ Trust me, I m a doctor: Examining changes in how privacy concerns affect patient withholding behavior, ” Journal of Medical Internet Research. 2017;19(1):e2. doi: 10.2196/jmir.6296.

[20] F. Gille, C. Brall, “ Limits of data anonymity: lack of public awareness risks trust in health system activities, ” Life Sci Soc Policy. 2021 Jul 26;17(1):7. doi: 10.1186/s40504-021-00115-9. PMID: 34304736; PMCID: PMC8310702.

[21] http://www.bredasturm.com/personal-data-protection-art-pdpa (access date: June 17th, 2023).

[22] https://digitallibrary.un.org/record/202686 (access date: June 17th, 2023).

[23] https://zdslu.si/majski-salon-2023-misterij-gea/ (access date: June 17th, 2023).

[24] J. Čebulj, 38. člen (varstvo osebnih podatkov)/Article 38 (Personal Data Protection), in: L. Šturm, Komentar Ustave Republike Slovenije, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002, p. 409.